

THE IMPACT OF COMPUTER PRIVACY CONCERNS ON ACCESS
TO GOVERNMENT INFORMATION

By

SIGMAN L. SPLICHAL

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

1993

ACKNOWLEDGMENTS

I thank the professors who served on my supervisory committee: Drs. Leonard Tipton and William McKeen from the University of Florida College of Journalism and Communications; Fletcher Baldwin of the UF College of Law; and Dr. Kermit Hall, dean of the College of Arts and Sciences at the University of Tulsa.

I owe a special debt of gratitude to Dr. Bill F. Chamberlin, Joseph L. Brechner Eminent Scholar in Mass Communication and chairman of my committee, for offering guidance, inspiration, and unstinting faith in me and my project throughout difficult times.

I also wish to thank Dean Ralph Lowenstein and Dr. Kurt Kent of the College of Journalism and Communications, Rick Donnelly and Rosalie Sanderson of the Legal Research Center, and reference librarian Dolores Jenkins.

I will never forget the help and good humor of Matt Bunker, my fellow graduate student, to whom I wish a successful career at the University of Alabama. My student days also were enriched considerably by the friendship of Dr. Judy McFetridge. My thanks to them both.

And finally, my love and heartfelt thanks go to my wife, Colee, and our son, Clark, for their support beyond measure.

TABLE OF CONTENTS

	<u>Page</u>
ACKNOWLEDGMENTS.....	ii
ABSTRACT.....	vii
 CHAPTERS	
ONE PRIVACY VS. ACCESS: THE ROLE OF THE COMPUTER..	1
The Importance of Access.....	1
The Issue of Privacy.....	6
The Scope of the Privacy/Access Issue.....	12
The Effects of Privacy Concerns on Access.....	16
A Framework for the Access/Privacy Conflict...	17
Contribution to the Literature.....	19
Definition of Terms.....	23
Notes.....	27
 TWO THE DEVELOPMENT OF SOCIAL AND LEGAL THEORIES SUPPORTING PRIVACY AND PUBLIC ACCESS TO GOVERNMENT INFORMATION.....	 32
A Right of Privacy.....	33
Privacy as a Social Value.....	35
Privacy as a Legal Concept.....	39
Constitutional Privacy.....	47
Legislative Recognition of a Right to Privacy...	58
A Right of Access to Government Information...	61
Toward a Theory of Self-Governance.....	62
Libertarian Underpinnings.....	63
Building on the Revolutionary Experience.....	65
Twentieth Century Legal Theory.....	68
A Common Law Right of Access.....	73
Access and the Constitution.....	74
The Right to Receive Information.....	77
A Right of Access to Government Information...	79
Statutory Access to Government Information....	86
State Access to Government Records.....	89
Privacy and Access in Conflict.....	90
Notes.....	92

THREE	THE EVOLUTION OF COMPUTER/PRIVACY CONCERNS: ACCESS TO GOVERNMENT INFORMATION HELD IN THE BALANCE.....	104
	The Core of the Debate.....	104
	Backdrop for the Computer/Privacy Debate.....	107
	The Computer Issue Unfolds in the Media.....	112
	Hearings on Creation of a National Data Center.....	120
	The Computer and the Bill of Rights Hearings..	132
	The Health, Education, and Welfare Report.....	138
	The Privacy Act of 1974.....	141
	The Computer Matching and Privacy Act.....	145
	Other Legislation Concerned About Computers and Privacy.....	151
	Fair Credit Reporting Act.....	151
	Fair Credit Billing Act.....	152
	Family Education Rights and Privacy Act.....	152
	Right to Financial Privacy Act.....	153
	The Computer Crime Act.....	154
	Electronic Communication Privacy Act of 1986..	155
	Computer Security Act of 1987.....	155
	Video Privacy Protection Act.....	157
	Scales Tipped Toward Caution.....	157
	Notes.....	159
FOUR	COURT CASES ADDRESSING PRIVACY CONCERNS ABOUT COMPUTERS.....	170
	A Question of Balance.....	170
	A Right of Informational Privacy?.....	173
	The Seeds of Informational Privacy.....	174
	The Supreme Court and Informational Privacy...	175
	A Seminal Case for Informational Privacy.....	183
	The Long Road to the Supreme Court.....	186
	A Definition of Informational Privacy.....	192
	A Public Record in the Computer Age.....	194
	Purpose of Disclosure.....	198
	Categorical Exemption of Information.....	203
	Cases Decided Since Reporters Committee.....	206
	Privacy-Access Cases Addressing Technical and Definitional Concerns.....	208
	Federal Courts and Technical and Definitional Privacy Concerns.....	209
	State Courts and Computer Access Issues.....	216
	Privacy/Access Out of Balance.....	227
	Notes.....	228

FIVE	TOWARD RESOLVING THE COMPUTER PRIVACY/ACCESS ISSUE.....	239
	Summarizing the Problem.....	239
	Access and Privacy: American Ideals.....	242
	When Values Collide.....	246
	A Model of Relative Values.....	248
	Relative Privacy Values.....	252
	Relative Access Values.....	256
	Application of the Model.....	264
	The Need for a Response.....	268
	Notes.....	272
	BIBLIOGRAPHY.....	276
	BIOGRAPHICAL SKETCH.....	291

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Philosophy

THE IMPACT OF COMPUTER PRIVACY CONCERNS ON ACCESS
TO GOVERNMENT INFORMATION

By

Sigman L. Splichal

August 1993

Chairman: Dr. Bill F. Chamberlin
Major Department: Mass Communication

This project explores how the growing computerization of government information is affecting the balance between personal privacy and public and media access to that information. The following questions are addressed, using legal and historical research to analyze court cases, legislation and legislative histories, and other sources: Have computer privacy concerns affected public policy and legislative activity related to government information practices? Have computer privacy concerns affected court opinions dealing with privacy-access issues? Have legislation and court opinions reduced, or threatened to reduce, access to computerized government information?

Analysis suggests concerns about computers and privacy run wide and deep, dating to a proposal in the early 1960s

for a National Data Center to pool information from various federal agencies. Computer privacy concerns raised during congressional hearings over the data center proposal eventually led to passage of the Privacy Act of 1974.

A review of court cases shows computers are raising novel issues, some of which are skewing the traditional balance between privacy and access to government information. Issues fall into three categories: technical and mechanical, interpretational and definitional, and public policy.

Technical and mechanical issues arise when access is reduced simply because a machine stands between the record keeper and the information requester and the record keeper is unable or unwilling to use the computer to effect access.

Interpretational and definitional problems related to access terminology and agency duties arise because most record laws and customs developed when government information existed primarily on paper. When the same information is in a computer, record keepers are not sure what responses are required to satisfy legitimate access requests.

Public policy questions have been centered on the nature of computerized information and whether it poses a greater threat to privacy than the same information in paper form.

The access/privacy issues raised when government information is in computers, and their potential threat to legitimate public and media access, indicate a need for legislatures to revisit access legislation to ensure it

remains viable. To this end, a descriptive model is proposed to show the relationship between access and privacy in the computer age.

CHAPTER ONE
PRIVACY VS. ACCESS: THE ROLE OF THE COMPUTER

The Importance of Access

The transistor was invented in 1947, the integrated circuit came along about 11 years later, and the modern computer epoch was born. That "mindless simpleton, but very fast mindless simpleton,"¹ forever altered how individuals and institutions, including governments, gather, store, sort, and analyze information.

Computers numbered fewer than three score among the federal agencies when California Congressman John Moss began hearings in 1955 that set the stage for passage of the Freedom of Information Act, a congressional recognition that the government's business was the people's business.² The Census Bureau had introduced the first government computer, a UNIVAC I, just four years earlier.³ Crude by the standards of the 1990s, these behemoth assemblages of hundreds of vacuum tubes and miles of electrical circuitry were novel, and their vast potential as information processors remained to be fully understood and exploited.

When President Lyndon Johnson signed the Freedom of Information Act on Independence Day, 1966, with the proclamation that "democracy works best when the people have

all the information that the security of the nation permits,"⁴ the federal government operated about 3,000 computers.⁵ Twenty years later, it maintained 22,000 large, mainframe computers; by 1990, that number had more than doubled to 48,000.⁶ Government use of smaller microcomputers increased from 490,000 in 1987 to more than a million two years later.⁷ In a scant three decades, computers and computer programming capabilities were refined and streamlined to the point that computer screens replaced the ubiquitous file cabinet as the dominant office fixture in an increasingly information-hungry society.

Along the way, the onslaught of computer technology has confounded many of the laws and customs affecting public and media access to government information that were established when most records had four corners and could be tucked into a filing cabinet. At the same time, the very existence of information in computers--its compactness and accessibility--has opened up a range of possibilities for involving the public in the democratic process, enhancing the ability of citizens to make informed decisions and to acquire more knowledge about the governments they elect to represent them.

The importance of an informed citizenry in a democratic society, discussed at length in Chapter Two, is deeply rooted in the American experience and has been a guiding force in twentieth century legislation and jurisprudence.⁸

The role of the citizen-elector was galvanized by the late Alexander Meiklejohn, the noted educator and former president of Amherst College. In elucidating the theory of freedom of expression, Meiklejohn strongly tied the importance of the free flow of information to self-governance. In his work Free Speech and Its Relation to Self-Government, published in 1948, Meiklejohn said the First Amendment's main purpose was to allow citizens to understand "the issues which bear upon our common life." He maintained that "no idea, no opinion, no doubt, no belief, no counterbelief, no relevant information" should be kept from the people. "Under the compact upon which the Constitution rests," he said, "it is agreed that men shall not be governed by others, that they shall govern themselves."⁹

Government information is a vital raw material for the press and an essential ingredient in a self-governed, democratic society. Much of the daily content of news broadcasts and publications is about government. But the task of keeping track of government goings-on is daunting. Newspapers, magazines, and broadcast stations in this country employ roughly 260,000 reporters and editors, many of whom in some way cover the activities of 17 million government workers. Although reporters attend press conferences, scour government documents, and have legions of sources within the bureaucracy, they still fall short of

covering the countless official decisions that are made and actions taken. Without a doubt, reporters--and the public--go unaware of many of them.¹⁰

With the unprecedented increase in government use of computers--and the media's comparatively recent abilities to gain access to millions of records on the large computers often used in government--a new kind of reporting has evolved that heretofore was not deemed possible. For example, St. Louis Post-Dispatch reporters George Landau and Tim Novak uncovered the fact dead people were voting in elections, by matching a computerized list of registered voters to a computerized list of death certificates. The computer was the all-important alternative to plowing through thousands of records--requiring an investment of time and manpower beyond the resources of many newspapers.¹¹

That improved access to computerized government information can lead to news stories that are more useful to the public is being demonstrated increasingly at computer-savvy newspapers around the country. Examples abound, among them the analysis of Internal Revenue Service files by the Transactional Records Access Clearinghouse in Syracuse, N.Y., which proved incorrect an IRS claim that underpayment of taxes had risen sharply during the previous 20 years. Computer analysis showed tax compliance rates had remained about the same since 1969.¹²

Similarly, when the National Transportation Safety Board said the maintenance record of a 25-year-old DC-9 that crashed in Cleveland was typical of any aircraft that age, a Cleveland Plain Dealer computer analysis of Federal Aviation Administration records showed a history of equipment malfunctions not found in similar planes.¹³

Such computer-assisted reporting, though around for more than a decade, came to the fore in 1989, when an Atlanta Journal and Constitution data base project showed widespread discrimination against blacks by home-mortgage lenders and won a Pulitzer Prize for investigative reporting. Since 1989, investigative projects involving computers have become the norm, resulting in additional Pulitzers for computer-assisted reporting. As Bill Dedman, the reporter who won the Pulitzer for the Atlanta stories, told News Inc., "Ten years from now . . . there won't be a term 'computer-assisted reporting.' It would be like saying pen-and-paper assisted reporting."¹⁴

Andy Schneider, whose efforts helped the Pittsburgh Press win back-to-back Pulitzer Prizes for stories based on computer analysis of government information, summed up the potential of the new technology another way: "It's not magic, but if you're willing to master the new technology, it's close."¹⁵

The initial successes of computer-assisted reporting are not without potential drawbacks. As record custodians

become more aware of the ability of reporters to probe government data bases, reporters could become victims of their own successes. Hard-hitting stories have shown record custodians that sophisticated analysis of computerized agency information can result in criticism of agency performance and practices. In some cases, this independent analysis of agency data has revealed problems not apparent to agencies themselves. For example, Newsday's Penny Loeb reported that New York City owed property owners \$275 million in tax overpayments and had failed to inform them. The city's finance department had provided her with computerized records, but the agency no longer was so forthcoming after the story appeared. "I've been in an eight-month battle for more tapes," Loeb told a news magazine.¹⁶

Common sense suggests that awareness of computer reporting capabilities by record custodians could result in some self-serving attempts to limit access. And socially and politically attractive arguments based on the costs of computer access, computer security, and privacy could foster attempts to foreclose access to information that previously has been publicly available, simply because it is contained in a computer.

The Issue of Privacy

Access to government information has never been an absolute; it always has involved balancing the social

benefits of public disclosure with competing social interests.¹⁷ While access undoubtedly yields substantial social benefits by informing the public about government and other important matters, values supporting access sometimes conflict with other equally important values, such as the privacy rights of individuals who interact with government and relinquish personal information in the process. The "rules" of this balancing process once yielded relatively predictable results when records were in paper format, and record custodians in comparison knew what was expected of them to fulfill requests for information lawfully. But most existing laws--including the federal Freedom of Information Act and similar state access statutes--are not adequate to acknowledge the presence of information in computers or deal with the increased demand by the public and press for such information.

Another, potentially more threatening challenge posed by computers is that their mere proliferation has stirred alarm at all levels of American life. This concern, first raised by the rampant growth of computers in the federal government during the 1960s, continues to be reflected in news stories of the 1990s, with disclosures and commentaries about the excesses of private data vendors who buy and sell personal information.¹⁸

When the computer was introduced to business and government, its star climbed steadily in the constellation

of historic innovations; a 1965 Time magazine cover story titled "The Cybernation Generation" quoted a General Electric vice president who proclaimed that "the electronic computer may have a more beneficial potential for the human race than any other invention in history."¹⁹ But as the computer's star rose, so also rose the specter of "Big Brother," the faceless, omnipresent technocrat in a society devoid of individualism and personal privacy, thrust into the lexicon in 1949 by George Orwell's unsettling novel 1984.²⁰ Orwell's villain was invoked during hearings in the 1960s over a proposal for a National Data Center to pool government data on individuals in a central computer. References such as "chains of plastic" and an "unforgiving god" abounded as discussion focused on the potential dangers posed by the vast accumulation of personal information by government bureaucrats.²¹

Computer privacy concerns continued into the 1970s, punctuated by passage of the Privacy Act of 1974. Pollster Louis Harris reported in a 1983 study, aptly titled The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life, that nearly half of those surveyed said they were "very concerned" about the threat computers posed to personal privacy. Sixty percent of the respondents favored drastic measures to ensure that computers did not erode privacy.²² The depth of support for strong constraints on

the new information technology impressed Harris, who observed,

Americans are not willing to endure abuse or misuse of information, and they overwhelmingly support action to do something about it. This support permeates all subgroups in society and represents a mandate for initiatives in public policy.²³

Indeed, the pervasiveness of computers in society has raised numerous legal and public policy issues related to privacy, both inside and outside of government. Many of these issues and problems--both practical and philosophical in nature--may threaten public and press access to government-held information. They have brought about--and could continue to result in--well-intentioned legislative and legal actions that endanger public access to government information.

Irony is inherent to this problem: While the public desires to be better informed about its government, and while the media now have more capability than ever to assemble and analyze that information (and more time and resources than any single citizen normally would have), fears for privacy may supersede all other concerns. Part of this fear is certainly based on a stereotype derived from popular culture, that of the anthropomorphic machine that takes over from the humans who have programmed it--and in some way goes awry. The idea is that if humans create machines in their own image, "play God," if you will, the consequences are disastrous. The scenario has been played

out from the dawn of the Industrial Age in Mary Shelley's novel Frankenstein through Stanley Kubrick's film "2001: A Space Odyssey" and beyond.²⁴

Fears were fanned in the early 1990s by the credit-reporting excesses, in which commercial vendors of computerized personal information were criticized for their mishandling of that information. Sometimes the abuse was in the form of incorrect computer entries that were allowed to self-perpetuate, adversely affecting the lives of individuals without their knowledge. Again, hovering around the discussion was the image of an implacable computer holding information that takes on a malevolent life of its own. Stories in publications ranging from The New York Times and Newsweek to American Demographics and the columns of James J. Kilpatrick and Jane Bryant Quinn noted this concern, offering proclamations from the experts that privacy was a hot issue.²⁵ Although the controversy in the early 1990s centered on the private sector, not government, worries about computer-held personal information were generalized. Newsweek reported Congress was scrambling to "bring some order to the hodgepodge of privacy and technology laws" and that the U.S. Office of Consumer Affairs was targeting privacy as one of its prime concerns, as were such advocacy groups as the Consumer Federation of America and the American Civil Liberties Union. Said

Janlori Goldman, head of the ACLU's Privacy Project,
"There's a tremendous groundswell of support out there."²⁶

In seeking protection from the watchful eyes of others or from any computerized compilation of personal information, however, lies the danger of muzzling the traditional watchdog of government, the press. Legislation and court interpretations could have the corollary effect of permitting government--in the name of protecting personal privacy--to hide information, cover up mistakes and excesses, obscure the governing process from the people.

The U.S. Supreme Court's 1989 opinion in Justice Department v. Reporters Committee for Freedom of the Press more than anything else has underscored the need for renewed legislative consideration of the privacy-access conflict.²⁷ The case ultimately involved attempts by a CBS correspondent and the Reporters Committee for Freedom of the Press to obtain prior arrest information, or "a rap sheet," on a principal in a business identified by the Pennsylvania Crime Commission as having ties with organized crime. The business also had been linked to a corrupt congressman. The information in question was compiled from public record sources in a Justice Department computer data base.²⁸

In allowing withholding of such information in a computer compilation, the Court articulated the "practical obscurity" doctrine, an acknowledgment of the social value of allowing individuals to put time and distance between

themselves and past mistakes. The Court concluded, among other things, that personal information--even information taken from public sources--enjoyed a reinvigorated privacy interest when drawn together in a government data base. The Court also held that such information could be categorically exempted from public disclosure, forgoing what had been the usual process of balancing particular privacy interests with the public interest in disclosure on a case-by-case basis.²⁹ In effect, the Court shifted the analysis away from the content of the information and its public-record status and focused instead on the computerized form of the information. The holding and legal reasoning of the Reporters Committee opinion are discussed at length in Chapters Four and Five.

For those in government who might wish to shield information from public scrutiny, the Court provided a potentially powerful weapon--based on the politically attractive rationale of personal privacy.

The Scope of the Privacy/Access Issue

Most privacy-access conflicts related to computers fall into three general categories: technical and mechanical issues, definitional or interpretational issues, and public policy issues. The general outlines of these issues, discussed at length in subsequent chapters, are presented below.

Technical and Mechanical Problems

Technical and mechanical problems related to computer privacy occur simply because the computer machinery--or hardware--stands between the record requester and the record custodian. Requesters who do not know how the machinery works frequently do not know the proper questions to ask to facilitate the release of disclosable information that is mixed with private, undisclosable information. On the other hand, record custodians often are not properly trained to respond to computer requests or are indifferent to the new technology (or perhaps use it as an excuse to withhold embarrassing information in the name of privacy) and, therefore, are unresponsive to legitimate information requests. For example, the Freedom of Information Act requires agencies to provide "reasonably segregable" portions of records that contain exempt private information mixed with disclosable information.³⁰ With paper records, exempt private information is simply blacked out before documents are provided. When records are in computers, custodians have used the computer as an excuse to deny access requests simply because they do not know how to segregate information stored in computer format, or they are unwilling to take the time or incur the cost. How courts have addressed these problems is examined in Chapter Four, which looks at legal opinions dealing with access-privacy issues.

Definitional or Interpretational Issues

Problems of definition and interpretation have occurred because most record-access laws and practices predate the widespread use of computers by government agencies. When the Freedom of Information Act was passed in 1966, most records existed in paper form. Paper also was the dominant record medium when most public access problems were sorted out, either by new legislation or by the courts. But laws and duties that were understood when most records were paper became muddled when the same kinds of records were held in government computers. And when laws and duties become muddled, they provide opportunities for government agencies to offer their own interpretations, sometimes motivated by administrative convenience or the desire to hide information rather than by legitimate privacy concerns.

The previous example of providing reasonably segregable portions of records is illustrative. In the paper era, agencies had learned through experience what constituted a reasonable response to requests for records that required the editing out of private information. But when records were computerized, it no longer was clear to agencies what constituted a reasonable response when exempt and nonexempt material were mixed in a computer data base. Are agencies in effect denying legitimate public access because they are reluctant to take time to operate or reprogram their computers to separate disclosable nonprivate information

from exempt private information? These questions are addressed in Chapter Four.

The Freedom of Information Act does not require agencies to create a "new record" to satisfy public record requests. But does the use of agency computers to separate disclosable and nondisclosable information constitute creation of a "new record"? Court cases discussing such problems of definition and interpretation also are studied in Chapter Four.

Public Policy Issues

Important public policy issues related to the widespread gathering and storage of personal information in government computers have arisen on a number of fronts. A fundamental concern involves the very nature of the computer and its role in a democratic society. The value of computers in improving government efficiency and cost effectiveness is beyond question. This societal benefit, in both the public and private sectors, is the driving force behind their widespread use. But, as witnesses during the National Data Center hearings asked, is the ability of computers to sort, compare, and analyze information with exacting efficiency itself an unwarranted threat to personal privacy that calls for further legal and public-policy analysis?³¹ Fear about the threat computers posed to personal privacy was expressed during the debate over whether to create a National Data Center and ultimately led

to passage of the Privacy Act of 1974 and other computer-related legislation. These hearings and legislation are discussed at length in Chapter Three. A generalized concern about computers and the danger they pose to personal privacy was the central issue in the Supreme Court's Reporters Committee opinion, mentioned previously.

A second public policy question involves the cost of computer technology and the extent to which agencies must invest in computer technology to ensure reasonable public and press access. Cost is a legitimate public policy consideration, but it also provides agencies with an attractive rationale for limiting access to computers. This question is discussed briefly in several court opinions in Chapter Four.

The Effects of Privacy Concerns on Access

The goal of this dissertation is to explore how the tension between the rampant growth of computer record systems in government and resultant privacy concerns is threatening public and press access to government-held information, an essential component of democracy. To this end, the dissertation employs legal research techniques, analyzing primary sources such as legal cases and legislation that reflect patterns and changes in the privacy/access equation. Historical research, tapping primary sources such as hearing transcripts as well as some secondary materials, also is used. Its role is to establish

the historical, social, and political contexts of some issues, and to delve into the legislative history of the privacy issue.

In addressing the proper balance between privacy and access, several questions are posed:

--How have computer concerns affected legislative activity related to personal privacy?

--To what extent have computer privacy concerns affected public policy regarding information in government computers?

--To what extent have computer privacy concerns affected court opinions dealing with privacy-access issues?

--To what extent have legislation and court opinions regarding access to computerized information reduced, or threatened to reduce, public and press access to government information?

It is hoped that attempting to answer these questions will help to determine what the proper course of action should be to protect privacy when appropriate without unnecessarily reducing public and media access to government information.

A Framework for the Access/Privacy Conflict

To establish a theoretical foundation from which to assess the impact of computer privacy concerns on access to government-held information, Chapter Two explores the philosophical, political, and legal roots of two important--

and sometimes competing--social values. The first is the right to personal privacy, which Supreme Court Justice Louis Brandeis has called simply "the right to be let alone."³² The second social value is the right of public and press in a democratic, self-governing society to have access to the information government uses to go about the people's business.

An overview of the tension between the sometimes-conflicting values supporting privacy and access to government information will provide the theoretical framework for discussing how legislators, government agencies, and the courts attempt to balance these values and to what effect.

Chapter Three attempts to trace the evolution of the federal government's concern about the threat of computers to personal privacy and to define the extent to which the federal government has responded to these concerns. The chapter looks at how various responses to computer privacy concerns have affected access to computerized information on individuals that the government gathers and disseminates. Chapter Four looks at how the courts have dealt with computer-privacy issues and at what these cases portend for public and press access when government information is held in computers.

Chapter Five attempts to construct a hierarchy of privacy and access values that could be used to help resolve

access/privacy questions. A model is proposed to help define a reasonable balance between privacy and public access. So that former levels of access--when laws pertained to records on paper--are maintained in the high-tech age, the model focuses on the content, not the form, of the information held by government. In doing so, the model looks at the kind of personal information involved, the likelihood that harm would result from disclosure, and the relative strength of the public good derived from disclosure.

This project also will propose the urgent need for a legislative response to prevent the reasoning of Reporters Committee and other computer-privacy cases from reducing public and media access to government information simply because information is held in a computer.

Contribution to the Literature

Much has been written about computers and the dangers they hold for personal privacy. Some works, such as Vance Packard's The Naked Society,³³ deal with general concerns about the effects of technological change on society and, when in the wrong hands, on civil liberties. Alan Westin's Privacy and Freedom³⁴ and Arthur Miller's The Assault on Privacy³⁵ are seminal books that greatly influenced early public debate when government agencies were just beginning to realize the capabilities of computers. Both authors played prominent roles in hearings that led up to the

Privacy Act of 1974. Westin and Miller and others, such as Richard I. Miller, wrote related articles for scholarly and legal journals and in the popular press dealing with the effects of technology on personal privacy.³⁶

Many substantial works have been written supporting public access to government-held records. Foremost among them is Harold Cross' The Right to Know.³⁷ Cross' work, sanctioned by the Society of Professional Journalists, influenced the debate that led to congressional recognition of the public's right to government information.

Several articles have been written about the overall effect computers are having on access to public information. Elliot Jaspin and Mark Sableman, for example, explore the significant changes wrought by the "new electronic government" in the traditional relationships between government and press. The authors conclude,

[T]he control and release of government computer-stored information is too important an issue to be left to the haphazard pattern of statutory and case law that has governed it to date. . . . Many of the existing decisions overemphasize general fears of the new electronic information-storage technology, and understate or ignore the great potential benefits of access to such information to the public.³⁸

Other articles state the urgent need for redefining the federal Freedom of Information Act in the face of burgeoning computer technology. Leo Sorokin, for example, calls on Congress to "broaden the definition of a record in the context of electronic information, enable FOIA requesters to

choose between paper and electronic formats, establish substantive criteria to determine when depository libraries should be provided access to on-line government databases, and direct that agencies provide the public with the benefits of computerization when agencies develop electronic dissemination programs."³⁹

Another author, Jerry Berman, envisions an "Electronic Freedom of Information Act," through which citizens can dial up the federal FOIA data base that has an index of agencies and subjects.⁴⁰ In the Jurimetrics Journal of Law, Science and Technology, Jamie Grodsky maintains "a broad, legislative message is needed to establish at least minimum requirements for agencies and give clearer guidance to the courts."⁴¹

Joining the chorus of advocates for better access to government information is Patti Goldman in Government Information Quarterly, but her perspective is that the Freedom of Information Act need not be tinkered with; instead, it is how the agencies interpret it that must be altered in the context of computer records. Instead of passing legislation tailored to electronic information, she suggests, Congress should "maintain vigilant oversight of agency practices to ensure that access to electronic information is provided to the public in accordance with the Act."⁴²

Matthew Bunker, Sigman Splichal, Bill Chamberlin, and Linda Perry, who devote some attention to the privacy/access nexus, propose computer-access criteria based on the assumption that access should not be restricted simply because records are in a computer. Among their 13 recommendations: Federal, state and local governments must promote public access needs when agencies install or upgrade computer systems, at which stage public access can be built in at little additional cost; all information in government-owned and operated computers must be a public record, absent specific statutory exemptions; and any agency using computerized records should make nonexempt information available through user-friendly computer terminals.⁴³

A host of other articles has examined how advancing technology has encroached on privacy, without focusing on how privacy concerns affect access. Among other things, the articles recommend individuals be informed in writing of the existence of identifiable information stored about them, the reasons it has been recorded, and the extent of its use by and dissemination to others. One author advocates amending the Privacy Act of 1974 to include predisclosure notification. Central to many of these articles seems to be the recognition that while computerized information is necessary for government efficiency, the individual must somehow retain some type of control over potentially harmful, identifiable information. In Computer/Law Journal,

C. Dennis Southard IV says courts must maintain a "minimum standard" of privacy based on the Fourth Amendment's guarantee of protection against unreasonable searches and seizures. "It should allow government to continue its police and national security protection at its current level, while guaranteeing that if an individual takes certain steps to assure his privacy, it will be respected,"⁴⁴ he reasoned.

None of the articles, however, looks specifically and in depth at how computer privacy concerns--both practical and philosophical--relate to public and media access to information held in government computers. It is this author's belief that by focusing on the question of how computer privacy concerns affect overall legitimate access to government-held information, the undertaking contributes to the scholarly discourse on one of the important social dilemmas in the information age.

Definition of Terms

Privacy has many dimensions, as the subsequent discussion of the evolution of the value will show. For the purposes of this dissertation, with its focus on access to government-held information, the type of privacy discussed will be informational privacy. The following definition of informational privacy, adopted by a congressional committee and later endorsed by the U.S. Supreme Court, will be used: "Privacy is the claim of individuals . . . to determine for

themselves when, how, and to what extent information about them is communicated to others."⁴⁵

The definition of government "information" also is central to this dissertation. For the purposes of this project, a definition provided by the U.S. Supreme Court in the 1980 case of Forsham v. Harris will be adopted. Borrowing terminology from the Federal Records Disposal Act, the court defined government information as

all books, papers, maps, photographs, machine-readable materials or other documentary materials, regardless of physical form or characteristic, made or received by an agency of the United States government under federal law or in connection with the transaction of public business.⁴⁶

No attempt is made to distinguish between government "information" and government "records," for to do so in the age of computerized information begs for circular reasoning. In this undertaking, they are assumed to be one and the same. The Colorado Supreme Court, in a 1986 computer access case discussed in Chapter Four, rejected an attempt to distinguish between "information" and "records." Said the court, "This is a distinction without a difference. Information does not exist in a vacuum. Rather a 'record' by its very nature exists to impart the information contained in it."⁴⁷

Various words and terms are used throughout this dissertation. To facilitate understanding, some key definitions follow.

Computer: A mechanical device that stores and processes information electronically. Computer systems are traditionally divided into three subclassifications: mainframe, mini, and micro. These divisions are related to the size of the computer and its speed of processing information.

Mainframe computer: A large, multitask computer designed to be operated simultaneously by multiple users.

Personal computer: A small, self-contained computer designed to be operated by one individual.

Computer hardware: The physical machinery used in the electronic computing process.

Computer software: The electronic instructions that tell a computer how to store information and manipulate it.

Computer data: Individual pieces of electronically stored information, such as names, addresses, Social Security numbers, etc., suitable for processing and interpretation.

Computer data base: An electronic collection of pieces of related data.

Computer input: Data entered into a computer system for storage or processing purposes.

Computer output: The conversion of electronic computer impulses into some usable format, such as computer tapes, disks, screen images, or printouts.

Computer system: The computer hardware, software, input devices, output devices, and auxiliary storage devices.

Computer program: Coded instructions that instruct a computer to complete a sequence of tasks to achieve a specific result.

Computer programming: The process for coding instructions so a computer can complete a specific task.

Computerized government information: The sum of all data in a government computer.

Computerized government records: Data in a government computer that have been organized in some fashion pursuant to a government or other function.

Public access to government information: Access predicated on any of several legal theories, primarily common law access and statutory access. A majority of the U.S. Supreme Court have never agreed that access to government information is a constitutional right.

Publicly accessible government information: All government-held information not specifically shielded from disclosure by statute.

Privacy: In most general terms, the right of individuals to be secure in their private lives and personal affairs. (Webster's New World Dictionary of the American Language, Second College Edition.) This general definition

encompasses informational privacy. (See Informational Privacy.)

Constitutional privacy: The right of individuals to be secure from intrusion by government into their private affairs. The U.S. Supreme Court has recognized this right in several areas: the right to be secure in one's home, the right of association, the right of intimate decision making, and the right to control information about oneself. (See Informational Privacy.)

Informational privacy: The right of individuals to control access to, and the dissemination of, personal information about themselves.

Notes

1. T.R. Reid, "Computerthink," 5 APF Reporter 7 (Winter 1983).

2. David Morrissey, "The Age of Electronic Government," presented at the 1990 Conference on Advanced Investigative Methods for Journalists 2 (1990).

3. John W. Macy Jr., "The New Computerized Age--4: Automated Government: How Computers Are Being Used in Washington To Streamline Personnel Administration--To the Individual's Benefit," Saturday Review, July 23, 1966, at 24. Macy points out that one of the first completely electronic computers ever built was called ENIAC, for electronic numerical integrator and calculator. It was built by the War Department and the University of Pennsylvania in 1946 to solve problems with ballistics research. The UNIVAC I was put into service by the Census Bureau in 1951 and was retired to the Smithsonian Institution in October 1963.

4. Thomas M. Susman, "Introduction to the Issues, Problems and Relevant Law" in "Your Business, Your Trade Secrets, and Your Government," 34 Admin. L.R. 117 (1982).

5. Morrissey at 2.

6. General Services Administration, Federal Equipment Data Center, Automated Data Processing Equipment in the U.S. Government (April 1990).

7. General Services Administration, Office of Federal Information Resources Management, Microcomputer Survey Report (September 1988).

8. See the Freedom of Information Act, 5 U.S.C. sec. 552; New York Times v. Sullivan, 376 U.S. 254 (1964).

9. Alexander Meiklejohn, Free Speech and Its Relation to Self-Government 88-89 (1948).

10. Elliot Jaspin and Mark Sableman, "News Media Access to Computer Records: Updating Information Laws in the Electronic Age" 36 St. Louis U.L.J. 351 (February 1992).

11. George Landau and Tim Novak, "Dead or Alive," St. Louis Post Dispatch, September 9, 1990, at 1A.

12. Katherine Corcoran, "Power Journalists," News Inc., November 1991, at 30. See also Mitchell Hartman, "Investigative reporters use databases to break stories," The Oull, November/December 1990, at 21-26.

13. Corcoran at 30.

14. Corcoran at 32. See also Howard Kurtz, "Reporters Let Their Terminals Do the Walking," The Washington Post, July 7, 1991, at F4.

15. Kurtz, supra note 14.

16. Katherine Corcoran, "Beating the Tape Resistance," News Inc., November 1991, at 30.

17. For example, Exemption 6 of the Freedom of Information Act allows withholding of information "that could reasonably be expected to cause an unwarranted invasion of privacy." This language contemplates a balancing of privacy interests with the public interest in disclosure.

18. See e.g., John Schwartz, "Consumer Enemy No. 1," Newsweek, October 28, 1991, at 42-47.

19. John W. Macy Jr., "The Cybernation Generation," Time, April 2, 1965, at 84.

20. George Orwell, 1984 3 (1949).

21. The Computer and Invasion of Privacy: Hearings Before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations, 89th Cong., 2d Sess. 12 (1966). See also Computer Privacy: Hearings Before the Subcommittee on Administrative Practices and Procedures of the Senate Committee on the Judiciary, 90th Cong., 1st Sess. 2 (1967).

22. See J. Kirchner, "Latest Harris Poll Uncovers Mixed Attitudes About High Tech," Computerworld, December 12, 1983, at 1, on the 1983 Louis Harris survey, The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life. See also "Sharp Increase in Concern" 16 Privacy Journal 7 (May 1990), citing other Harris surveys noting privacy concerns among the population. See also John Schwartz, "How Did They Get My Name?" Newsweek, June 3, 1991, at 40-42. A 1990 Harris poll taken for consumer-data conglomerate Equifax showed that 79 percent of the respondents were worried about threats to their privacy, up from 47 percent in 1977.

23. Id.

24. 2001: A Space Odyssey (Metro-Goldwyn-Mayer 1968). In the movie, a computer named HAL takes over a space station from two astronauts.

25. See e.g., Jane Bryant Quinn, "Guarding Your Good Name," Newsweek, August 12, 1991, at 64.

26. Schwartz, supra note 22 at 40.

27. Justice Department v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

28. Id.

29. Id.

30. Freedom of Information Act, 5 U.S.C. sec. 552(b).

31. See generally The Computer and Invasion of Privacy, supra note 21.

32. Olmstead v. United States, 227 U.S. 438, 478 (1928).

33. Vance Packard, The Naked Society 3-43 (1964).

34. Alan F. Westin, Privacy and Freedom (1967).

35. Arthur Miller, The Assault on Privacy (1971).
36. See Richard I. Miller, "Data Banks and Privacy," in Computers and the Law: An Introductory Handbook 156-161 (R.P. Bigelow 2d ed. 1969).
37. Harold Cross, The People's Right to Know (1953).
38. Jaspin and Sableman, supra note 10 at 405, 404.
39. Leo T. Sorokin, "The Computerization of Government Information: Does It Circumvent Public Access Under the Freedom of Information Act and the Depository Library Program?" 24 Colum. J.L. & Soc. Probs. 297 (1990). See generally Sandra Davidson Scott, "Computer Technology v. Laws on Access," unpublished paper presented to the Association for Education in Journalism and Mass Communication annual convention, Boston, Mass. (August 1991).
40. Jerry J. Berman, "The Right To Know: Public Access to Electronic Public Information," 3 Software L.J. 523 (Summer 1989).
41. Jamie A. Grodsky, "The Freedom of Information Act in the Electronic Age: The Statute Is Not User Friendly," 17 Jurimetrics J. 51 (Fall 1990).
42. Patti A. Goldman, "The Freedom of Information Act Needs No Amendment to Ensure Access to Electronic Records," 7 Gov't Info. O. 400 (1990).
43. Matthew D. Bunker, Sigman L. Splichal, Bill F. Chamberlin, and Linda M. Perry, "Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology," 20 Fla. St. U.L. Rev. 594-598 (Winter 1993).
44. See generally Louise M. Benjamin, "Privacy, Computers, and Personal Information: Toward Equality and Equity in an Information Age," 13 Comm. & the L. 3-16 (June 1991); C. Dennis Southard IV, "Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information," 9 Computer/L. J. 359 (Summer 1989); Fred W. Weingarten, "Communications Technology: New Challenges to Privacy," 21 J. Marshall L. Rev. 735 (1988); Donsia Renee Strong, "The Computer Matching and Privacy Protection Act of 1988: Necessary Relief from the Erosion of the Privacy Act of 1974," 2 Software L. J. 391 (Summer 1988).
45. Reporters Committee at 763.

46. Forsham v. Harris, 445 U.S. 169, 183 (1980).

47. Western Services, Inc. v. Sergeant School District
No. RE-33J, 719 P.2D 355, 358 (Colo. App. Jan. 2, 1986).

CHAPTER TWO
THE DEVELOPMENT OF SOCIAL AND
LEGAL THEORIES SUPPORTING PRIVACY
AND PUBLIC ACCESS TO GOVERNMENT INFORMATION

The public's "right to know"¹ about the business of government and individuals' "right to be let alone"² are fundamental to American society, each firmly anchored in the mores and values that have guided the development of the nation. But these rights are not mutually exclusive. The rights of the public and media to know about government through access to the information it gathers--derived from historical and twentieth century philosophical principles of a free press and a self-governing democracy--are not absolute. Neither are the rights of individuals to be shielded from unwanted intrusions into their personal affairs. Each of these rights, which the Supreme Court has recognized are "plainly rooted in the traditions and significant concerns of our society,"³ on occasion imposes limits on the other, and at times they come into conflict as the news media go about the task of informing the public about matters of concern.

This chapter charts the development of a free press in self-governing American society with its need for access to government information, and the development of the concept

of personal privacy. It highlights the legal, philosophical, and historical roots of each. The chapter shows how rights of access and privacy have clashed from time to time because of social, economic, and technical change, causing friction between legitimate free-press and personal-privacy interests. The chapter concludes by introducing the most recent social and technological developments that have brought privacy and access into conflict--the government's use of computers and its burgeoning need for personal information to make policy and provide benefits to citizens. Subsequent chapters will explore legislative and judicial concerns about the effects of computers on privacy and how such concerns threaten public and media access to the information government uses to make decisions.

A Right of Privacy

U.S. Supreme Court Justice Arthur Goldberg, in an attempt to explain the origin and dimensions of a right of privacy, has suggested a fruitful approach for assessing society's values. In his concurring opinion in Griswold v. Connecticut in 1965, a case that fashioned a constitutional right of privacy, Justice Goldberg concluded that privacy was among those unenumerated rights retained by the people under the Ninth Amendment to the Constitution.⁴ The Ninth Amendment states that the failure of the Constitution to recognize a particular right does not mean that no such

right exists; rather, the amendment concludes that important rights not mentioned in the document are assumed to be retained by the people. To determine whether a particular right was among those retained by the people under the Ninth Amendment, Justice Goldberg reasoned that it was necessary to look at it in the social and political context of the American experience. He said that one "must look to the tradition and [collective] conscience of our people [and at] . . . the totality of the constitutional scheme under which we live."⁵

Without passing judgment on Justice Goldberg's Ninth Amendment rationale for a constitutional right of privacy, the following discussion of access and personal privacy attempts to use his basic approach to explore the traditions and conscience of the nation within "the constitutional scheme under which we live." In doing so, the discussion traces the development of a right of privacy under common law, the unwritten law based on custom or court decision; constitutional law; and statutory law. It is hoped that this discussion, along with subsequent study of cases, laws and political theories supporting a right of access to government information, will provide a framework within which to explore the ongoing tension between computers and personal privacy and how this conflict affects public and media access to government information.

Privacy as a Social Value

The seeds of privacy can be traced to the beginning of the Judeo-Christian era in the biblical book of Genesis. Ever since the story of Adam and Eve, who were shamed in the eyes of God and took refuge behind fig leaves, modesty has been a basic social and religious value integral to the modern concept of privacy. After Adam and Eve defied God and ate from the tree of knowledge, "the eyes of both were opened, and they knew they were naked." Genesis further noted that "God made for Adam and his wife coats of skins, and clothed them."⁶ Modesty has played a central role in the development of various cultures in the millennia since Adam and Eve stepped from the Garden of Eden into a world governed by human nature.⁷

A concept of privacy, though never expressed as it is understood today, was not unknown in English common law, the legal system dominant in colonial America and later adopted by the fledgling nation. English common law cases dating back to the Norman conquest recognized a value resembling privacy in property rights of individuals.⁸ The case of Pope v. Curl in 1741 illustrates the approach the English common law followed. To resolve the case, the House of Lords, England's highest court, applied a property-rights doctrine to protect the contents of individuals' personal letters from unauthorized publication by others.⁹ This case was important to development of privacy in American

jurisprudence because it acknowledged a property right in individuals' retention and control of personal ideas contained in letters sent to others, not only in the letters themselves.

In the development of American social and legal values, the basic characteristics that embody the modern legal concept of privacy predate the American Revolution. Philosopher John Locke, whose writings influenced the libertarian sentiments of the Founding Fathers' generation, argued that government had a duty to protect certain fundamental rights, such as life, liberty, and property.¹⁰ These "inalienable rights" would find expression in the Declaration of Independence, the Constitution, and the Bill of Rights, and the Supreme Court almost 200 years later would glean from the fundamental concept of liberty a constitutional right of privacy.¹¹

John Adams, writing in his diary during the nation's formative years, extolled the virtues of privacy when he reasoned there was some personal information about which "others have not a Right to Know." Adams, who would become the nation's second president, maintained individuals should dissimulate--or protect their feelings or motives--because such information in the wrong hands could result in personal harm. Said Adams,

The first Maxim of worldly Wisdom, constant Dissimulation, may be good or evil, as it is interpreted. If it means only a constant concealment from others of such of our Sentiments,

Actions, Desires, and Resolutions, as others have not the Right to Know, it is not only lawful but commendable because when these are divulged, our Enemies may avail themselves of the Knowledge of them. . . . Things that ought to be communicated to some of our Friends, that they may improve them to our Profit or Honour or Pleasure, should be concealed from our Enemies, and from indiscreet friends. . . . This kind of Dissimulation, which is no more than Concealment, Secrecy, and Reserve, or in other words, Prudence and Discretion, is a necessary Branch of Wisdom.¹²

In his book Privacy in Colonial New England, historian David H. Flaherty explored the precursors of modern privacy, which he found evident during the American colonial experience. These precursors include such concepts as solitude, intimacy, anonymity, and reserve.¹³ Flaherty observed that although a right of privacy as a legal doctrine evolved slowly in Western culture, its underlying values were expressed in colonial customs and in the courts. Colonial courts, he suggested, protected privacy values indirectly by enforcing laws against trespass or physical intrusions, by limiting government searches and seizures, by hearing defamation cases, and by recognizing privileged communications between wives and husbands.¹⁴ Ironically, as Flaherty pointed out, there was little physical privacy--in the modern sense--within most homes and public inns. Homes often lacked individual sleeping quarters, and families congregated in common beds. Communal sleeping arrangements also were a common feature in public accommodations. Flaherty noted that the concept of informational privacy was officially recognized during Benjamin Franklin's tenure as

postmaster general before the American Revolution. During this time, postmasters were required to swear an oath that they would not "wittingly, willingly, or knowingly open or cause, procure, permit, or suffer to be opened . . . any letter or letters which shall come into their hands."¹⁵

Flaherty also maintained that values supporting privacy during the colonial period were instrumental in the formulation of the First, Fourth, Fifth and Ninth amendments to the U.S. Constitution.¹⁶

Values underlying privacy were apparent as the Revolutionary War drew near, and played a central role in the colonists' growing hostility toward British rule. In 1761, Boston lawyer James Otis, speaking out against the practice of general searches by the colonial rulers, noted, "Now one of the most essential branches of English liberty, is the freedom of one's own house. A man's house is his castle; and while he is quiet he is as well guarded as a prince in his castle."¹⁷

On the eve of the Revolutionary War, each colony drew up a list of grievances against the British authorities. Atop each list was concern about general warrants, which authorized government officials to search premises at will, without first presenting evidence of a specific violation of the law. After the colonies won independence, James Madison, the major proponent of a Bill of Rights spelling out individual liberties, introduced a proposal during the

Constitutional Convention in 1789 to limit the scope of government searches. He argued that a Bill of Rights to the Constitution was necessary to ensure, among other things, that the new government could never attempt to enforce general search warrants, so loathed by the colonies before independence.¹⁸ Madison's proposal, which established "the right of the people to be secure . . . against unreasonable search and seizures," was later adopted as the Fourth Amendment.¹⁹

Values supporting privacy also found expression in the writings of nineteenth-century philosopher John Stuart Mill, whose works were widely read in the United States. In Mill's influential work On Liberty, he argued the government should have no say in certain kinds of personal conduct, absent a compelling social interest, such as preventing harm to others. Expounding on this concept of personal "liberty," Mill wrote,

The sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number is self-protection. That is the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. . . . The only part of conduct of anyone for which he is amenable to society is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute.²⁰

Privacy as a Legal Concept

While Flaherty documented the existence of the components of privacy during the nation's formative years,

privacy as an identifiable legal concept remained only an undercurrent in the common law during the nation's first century. Legal concerns related to privacy developed slowly, in large part because of the agrarian nature of society. People were relatively few and far between, and this measure of physical distance reduced the potential for unwanted contacts and physical intrusions and the need for legal solutions. Yet, court cases reflecting privacy concerns did surface in the common law. One nineteenth-century case worth mentioning because of its unusual facts is Demay v. Roberts.²¹ The case, decided by the Michigan Supreme Court, arose when a doctor took an untrained assistant with him to help deliver a baby. The parents sued when they learned the assistant was not medically trained; they claimed their privacy had been compromised. The court agreed, holding that the mother had a "legal right to the privacy of her apartment at such a time."²²

The demographics of agrarian American shifted dramatically as the American industrial revolution hit full stride. Technological developments such as the steam engine led to the growth of manufacturing-based cities populated by factory workers. Physical distance separating individuals and families shrank as people moved to the cities to work in the factories or immigrated to the growing nation in search of opportunity. In the crowded cities, the natural barriers of time and space common to agrarian settings no longer

insulated individuals from unwanted contacts and intrusions.²³ Between 1870 and 1900, the population of the United States doubled and the number of urban residents tripled.²⁴

Dramatic technological developments during the nineteenth century that threatened personal privacy are traced by Alan F. Westin in Privacy and Freedom, a comprehensive study of privacy-related issues.²⁵ As Westin noted, "Three technological developments in the late nineteenth century altered the balance between personal expression and third-party surveillance that had prevailed since antiquity."²⁶ These innovations included the microphone and the telephone in the 1870s, the Kodak camera with its potential for "instantaneous photographs" in the 1880s, and the dictograph recorder in the 1890s.

In 1877, The New York Times expressed concern about the effect of new technology on privacy. In one of several editorials about privacy the newspaper would write in the coming years, the Times took issue with the telephone--a "nefarious instrument" with its "vast capabilities for mischief" that promised to rob individuals of their personal privacy.²⁷ Responding to a decision by the city to allow telephone wires to be attached to city lampposts, the Times cautioned,

Every confidential remark made to a lamp-post by a belated Democratic statesman could be reproduced by a telephone connected with any other lamp-post. . . . Men who had trusted to friendly lamp-posts,

and embraced them with the utmost confidence in their silence and discretion, would find themselves shamelessly betrayed, and their unsuspecting philosophies literally reported to their indignant families.²⁸

While technological innovations led to growth of populous industrial cities and such privacy-altering inventions as the telephone, other innovations--in the form of high-speed newspaper presses and advanced photography--spawned an aggressive new kind of journalism, a distant cousin of the Colonial and Revolutionary printers who catered to the well-read and politically astute of society. New printing processes could produce newspapers quickly and cheaply, and a new kind of journalism developed that often directed its content at the baser instincts of the swelling numbers of city dwellers. A new breed of mass newspaper reader, not so interested in the complexities of politics and other public issues, sought more information about the misdeeds and travails of others. This new kind of readership, coupled with the ability of journalists armed with cameras to intrude into areas previously shielded by lack of technology, sometimes brought newspaper practices and privacy concerns into conflict. This conflict created new social and legal issues to be sorted out, such as the rights of individuals to choose not to appear on the pages of local newspapers.²⁹

In 1890, a pair of former law partners and Harvard Law School classmates took issue with the newspaper practices

and new technologies of the day. Louis Brandeis and Samuel D. Warren, uppercrust Boston lawyers, penned "The Right to Privacy" for the Harvard Law Review.³⁰ The seminal article would steer the concept of a legal right of privacy toward the mainstream of American jurisprudence. Attempting to document a climate of journalistic excesses and abuses of privacy, the article stated somewhat hyperbolically that "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"³¹

Brandeis and Warren argued that individuals possessed certain intangible attributes, such as sentiments and intellect, over which they exercised rights akin to those governing personal property. The authors identified these rights in what they viewed as analogous laws on breach of trust, assault, copyright, and defamation, among others. The article arguably achieved its aim of bringing privacy into the legal arena.³² In 1891, soon after "The Right to Privacy" was published, the New York Supreme Court addressed the "novel" issue of personal privacy. Said the court, "It is true that there is no reported decision which goes to this extent in maintaining the right of privacy, and in that respect this is a novel case."³³

The case, Schuyler v. Curtis, arose when the family of a prominent woman filed a suit against a private organization, challenging its plans to erect a life-size statue in her memory. The family argued that the woman had never been a public personality and that the statue constituted an invasion of privacy. The court, noting the case before it was a test case for the right of privacy, rejected the family's claim. But the court stopped short of fully exploring the privacy issue. Important to the court's analysis was the fact the subject of the statue was dead. The court noted that, whatever right of privacy the woman had, it followed her to the grave. The extent to which a living person might have asserted a legally enforceable privacy right was not explored.

In some early privacy cases, courts showed a willingness to consider the interests of the press. For example, in 1902 the New York Court of Appeals, the state's highest court, refused to recognize a distinct right of privacy in Roberson v. Rochester Folding Box Co.³⁴ The case began when the family of a young girl sued the Franklin Mills Company for using a photograph of the girl without permission in an advertisement for the company's flour. The advertisement referred to the girl as "The Flour of the Family" and was posted in various public places. The family claimed invasion of privacy and argued that the advertisement caused the girl to be "greatly humiliated by

the scoffs and jeers of persons who recognized her face and picture."³⁵

The court, while sympathetic to the girl's predicament, nonetheless refused to recognize a legal remedy for an injury that was not physical. The court expressed concern that recognizing the claim might trigger similar lawsuits that would clutter the courts and place unreasonable burdens on the press. The girl's plight and controversy surrounding the court's action was not lost on the New York Legislature. In response, the legislature adopted a law creating a civil remedy for the use of a person's name or likeness for commercial purposes without consent.³⁶

While the New York court was unwilling to recognize a legal right of privacy, the Georgia Supreme Court not long afterward reached the opposite result in a similar case. In Pavesich v. New England Life Insurance Co., Georgia's high court became the first to recognize unauthorized commercial use of one's identity as a violation of the person's right of privacy.³⁷ The Georgia opinion prompted Louis Brandeis to write that he was encouraged to see that privacy as a distinguishable legal right was being recognized by the courts.³⁸

In addition to promoting privacy as a legal doctrine, the article by Brandeis and Warren in the Harvard Law Review also may have helped elevate the right of privacy to the level of public discourse. In 1902, The New York Times took

issue with the new photographic technology, which no longer required a willing subject to sit motionless to be photographed. The newspaper complained in an editorial, echoing the concerns of Brandeis and Warren, that "'kodakers lying in wait' to photograph public figures had become a 'wanton' invasion of privacy that demands legal control."³⁹

While the Brandeis and Warren article arguably nudged the issue of a right of privacy onto the social and legal stage, the development of a unified legal theory supporting a right of privacy remained elusive. In the following decades, the legal contours of privacy developed piecemeal and with many variations.

Seventy years after "The Right to Privacy" proposed a separate legal remedy for invasion of privacy, William Prosser summarized the extent of common law development of the privacy tort in the California Law Review. The 1960 article, titled simply "Privacy,"⁴⁰ dealt only with tort law and not with the constitutional question of government interference in private matters. After reviewing some 200 privacy-related cases, Prosser identified four separate torts--or breaches of duties imposed by society that resulted in harm to another individual. They were disclosure of embarrassing private facts about individuals; appropriation, or the use of a person's name or likeness without permission; false light, the intentional dissemination of highly offensive false publicity about

another; and intrusion, the physical or technological violation of an individual's privacy.

Prosser, an authority on tort law and author of a seminal treatise on the subject, further defined the private facts tort as publicity of a private matter that would be highly offensive to a reasonable person and not of legitimate public concern.⁴¹ Prosser's definition, especially its reference to matters of "legitimate public concern," highlights the factors courts traditionally have weighed in balancing personal privacy with the media's right to publish some kinds of personal information. Implicit in the definition is that a legitimate public interest in personal information could overcome privacy rights, even when disclosure would offend most people. The privacy-public interest balancing suggested by Prosser's definition is addressed more thoroughly in subsequent discussions of statutory privacy and court cases attempting to strike such a balance.

Constitutional Privacy

While common law privacy developed gradually in America over more than two centuries, explicit Supreme Court recognition of a constitutional basis for personal privacy occurred only in recent decades, beginning with the landmark case Griswold v. Connecticut in 1965.⁴² Unlike the common law tort, which gives individuals the right to sue other individuals or entities for violations of their privacy, a

constitutional right of privacy protects individuals from actions by the federal government and the states.

The Supreme Court's recognition of constitutional privacy can be broken down into four general categories: privacy from unwarranted intrusions, privacy of association, privacy in making intimate decisions, and privacy in controlling personal information. The first category involving Fourth Amendment cases of physical and electronic intrusion is well developed. The second and third categories also are reasonably well developed. They are associational privacy, or the freedom from interference or constraints on relationships with groups or individuals, and decisional privacy, or freedom from government interference in intimate personal decisions. The fourth area in which the Supreme Court has recognized a constitutional privacy interest is less developed. It concerns informational privacy, or rights of individuals to control information about themselves. It imposes a duty on government to protect the privacy rights of individuals on whom it gathers, keeps, or disseminates information.

Freedom from Unwarranted Intrusion

The first and oldest judicial recognition of privacy involves search and seizure cases implicating the Fourth Amendment, usually resulting from physical intrusion. The 1886 case Boyd v. United States is illustrative.⁴³ In Boyd, the Court said the Fourth Amendment search and seizure

provision voided a federal statute that required importers to relinquish business records for seized goods or forfeit the goods. The opinion, which expressed privacy values the Court would expound on over the next 100 years, said, "It is not the breaking of [an individual's] doors and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of the indefeasible right of personal security, personal liberty and private property."⁴⁴

The Court has recognized privacy as freedom from unwarranted intrusion in a number of other Fourth Amendment cases. During the twentieth century, several Supreme Court cases involving Fourth Amendment claims addressed threats to personal privacy made possible by new technologies--a theme introduced in the latter decades of the nineteenth century.⁴⁵ Thirty-eight years after publication of "The Right to Privacy" in the Harvard Law Review, Louis Brandeis, by then a U.S. Supreme Court justice, took issue with the majority of the court's upholding of the government in a telephone wiretapping case. In his oft-quoted dissenting opinion in Olmstead v. United States, Justice Brandeis said,

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, as against the government, the right to be let alone--the most comprehensive of rights valued by civilized men. To protect that right, every unjustifiable intrusion by the government on the privacy of the individual . . . must be deemed a violation of the Fourth Amendment.⁴⁶

In another Fourth Amendment case a dozen years later, Justice Murphy took up Brandeis' argument that Olmstead had been wrongly decided. In Goldman v. United States, a case involving the surreptitious use of an electronic listening device by government agents, Justice Murphy launched the concept of privacy into the technological age. He conceded that no physical intrusion or search had taken place. But he warned, "Science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment."⁴⁷ The court underscored the privacy value embodied in the Fourth Amendment in the landmark case of Mapp v. Ohio. The case established the exclusionary rule, which made evidence obtained during an unlawful search inadmissible in courts.⁴⁸ The court held that

Having once recognized the right of privacy embodied in the Fourth Amendment is enforceable against the states and that the right to be secure against rude invasions of privacy by state officers is, therefore, constitutional in origin, we can no longer permit that right to remain an empty promise.⁴⁹

Associational Privacy

The Supreme Court has invoked the First Amendment's free speech and free association clauses to carve out a right of associational privacy. The Court first applied a First Amendment rationale to protect a privacy relationship in the 1958 case NAACP v. Alabama ex rel. Patterson.⁵⁰ The

National Association for the Advancement of Colored People challenged a court order that the civil rights organization turn over to the state of Alabama its membership rolls. The NAACP argued that such information might be used to intimidate members and, consequently, discourage membership. Writing for the unanimous court, Justice Harlan said the Court "has recognized the vital relationship between freedom to associate and privacy in one's association . . . particularly where a group espouses dissident beliefs."⁵¹ Two years later, the Court again addressed the issue of associational privacy. In Shelton v. Tucker, the court narrowly struck down an Arkansas statute requiring schoolteachers to disclose all organizations to which they belonged, or contributed, during the previous five years. The Court was concerned that public access to records of teacher affiliations might lead to the harm of teachers who listed controversial or unpopular organizations.⁵² As the Tucker opinion shows, the Court at least to some degree agreed with John Adams' assertion that there are some matters about which "the public has not the Right to Know."⁵³ These associational privacy cases are also important to the access-privacy discussion because the Court recognized the potential for serious harm to individuals who lose control of personal information about themselves. This recognition will become more apparent in subsequent discussion of informational privacy cases.

Decisional Privacy

Many of the Supreme Court's first forays into the uncharted waters of constitutional privacy occurred before the turn of the century in cases that focused on the "liberty" rights of individuals in making certain kinds of economic decisions.

The 1897 case Allgeyer v. Louisiana⁵⁴ presaged reasoning the court would apply in decisional privacy cases more than a half century later. In Allgeyer, the Court struck down a statute that limited the authority of insurance companies to enter into certain contracts.⁵⁵ The court held that the "liberty" interest protected by the Fourteenth Amendment due process clause "means not only the right of the citizen to be free from physical restraint" but also from government interference in individual decisions.⁵⁶

The Supreme Court reached a similar result in the 1923 case Meyer v. Nebraska when it overturned the conviction of a teacher who taught a foreign language to schoolchildren in violation of a state statute.⁵⁷ The case was decided in the lower courts on the premise that the courts should protect the economic freedom of private schools. However, the issue as the Supreme Court posed it was one of freedom of inquiry and thought. Again, the Court noted that "liberty" meant more than "merely freedom from bodily restraint but also the right of individuals . . . generally to enjoy those

privileges long recognized at common law as essential to the orderly pursuit of happiness by free men."⁵⁸

In the 1925 case Pierce v. Society of Sisters, the Supreme Court applied the reasoning of Meyer to void a statute requiring children to attend public schools. The Court said the statute interfered with the "liberty of parents and guardians to direct the upbringing and education of children under their control."⁵⁹ Under this reasoning, a government cannot interfere with parents' decisions about whether their children will attend public or private schools. However, once the parents opt for the privilege of sending their children to public schools, the freedom of choice diminishes dramatically.

The Supreme Court has articulated its strongest recognition of a constitutional right of privacy in more recent decisional privacy cases, those involving freedom of choice in intimate personal decisions. The Court's clearest articulation of a right of decisional privacy came in Griswold v. Connecticut, a 1965 case that struck down a statute that made it a crime for anyone, including married people, to use contraceptives.⁶⁰ In Griswold, the court held that the statute intruded on the intimate relationship of married couples and violated a "zone of privacy created by several fundamental constitutional guarantees."⁶¹

The rationales for voiding the statute varied, but six justices agreed it violated the due process clause of the

Fourteenth Amendment by interfering in couples' intimate decisions on whether or not to use contraceptives. Specific mention of a right of privacy appears nowhere in the Constitution or the Bill of Rights. However, Justice Douglas, writing the primary opinion for the Court, found justification for a constitutional right of privacy in the "penumbra" of rights associated with the First, Third, Fourth, Fifth, and Ninth amendments. Justice Douglas said that "specific guarantees in the Bill of Rights have penumbras, formed by emanations . . . that give them life and substance."⁶²

In a concurring opinion, Justice Harlan provided another rationale for a right of privacy that recognized that privacy concerns at times must be balanced with broader societal demands. Relying on his dissent in an earlier case, Poe v. Ullman, he concluded that the Connecticut statute violated privacy values "implicit in the concept of ordered liberties."⁶³ Harlan, looking back at how the Court historically had attempted to balance personal liberties with other societal values, reasoned,

Due process has not been reduced to any formula. The best that can be said is that through the course of the Court's decisions it has represented the balance which our Nation, built upon the postulates of respect for liberty of the individual, has struck between that liberty and the demands of organized society.⁶⁴

In 1973, the court underscored the right of individuals to make intimate decisions in Roe v. Wade, a controversial

case involving a woman's right to decide whether to have an abortion.⁶⁵ In Roe, as in Griswold before it, the Court held the government to a standard of strict scrutiny when government attempted to interfere in intimate decisions. Under the strict scrutiny standard, the government must show a compelling interest in regulating a particular activity and that the means of regulating the activity are narrowly tailored to achieve the interest.

Informational Privacy

The most recent privacy concept recognized by the Supreme Court is informational privacy. Concerns about privacy have been raised in several cases addressing government use of computers to gather, store, and disseminate information about private individuals. The Supreme Court's approach to informational privacy is discussed briefly below and will be explored in more depth in Chapter Four, which focuses on how courts have dealt with both practical questions and public policy issues related to privacy and access to information held in government computers.

Concern about the impact of new information processing technologies on privacy was first expressed on the Supreme Court in 1976 by Justice William Brennan in a dissenting opinion in United States v. Miller.⁶⁶ The Miller majority held that an individual did not have a constitutional privacy interest in personal information voluntarily given

to a bank, because the information had become a part of the bank's business records. Justice Brennan, signaling a growing concern on the Court about the threat of information technology to personal privacy, cautioned, "Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the abilities of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds."⁶⁷

A year later, in Whalen v. Roe, the court acknowledged a right of information privacy in an opinion that said a New York state practice of compiling and storing in a computer certain prescription drug records on individuals did not violate their constitutional right of privacy.⁶⁸ Central to Justice Stevens' majority opinion were the "strong security provisions" imposed by the state to ensure privacy.⁶⁹ Said Justice Stevens, "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."⁷⁰

Justice Brennan, in a concurring opinion echoing concerns about the threat of computers to privacy, noted prophetically, "The central storage and easy accessibility of computerized data vastly increases the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity for some curb on such technology."⁷¹

After Whalen v. Roe, several informational privacy cases reached the U.S. Courts of Appeals, but none reached the Supreme Court until United States Department of Justice v. Reporters Committee for Freedom of the Press in 1989.⁷² In Reporters Committee, decided almost a century after Brandeis and Warren first took issue with the encroachment of technology on personal privacy, the Supreme Court apparently deemed that "the necessity of some curb" on modern computer technology was in order.

The case stemmed from a Freedom of Information Act request to the Federal Bureau of Investigation for computerized criminal history records that had been compiled from public records. In upholding the FBI's denial of the request, Justice Stevens reasoned,

the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interests implicated by disclosure of that information. Plainly, there is a vast difference between the public records that might be found after a diligent search of the courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearing house of information.⁷³

In his discussion of the case, Justice Stevens also adopted a definition of privacy that included the control by individuals of personal information about themselves.⁷⁴ The implications for public and media access as a result of the Reporters Committee reasoning, and subsequent cases based on that reasoning, will be explored in Chapter Four, along with

state cases that reflect concerns about the privacy threat of computerized information.

Legislative Recognition of a Right to Privacy

While the concept of informational privacy has been embraced by the Supreme Court, the clearest statements of privacy rights in information collected by the government have come through the legislative process. Most of the legislative concern has been in response to the growing use of computers by government. The evolution and dimensions of that legislative interest will be discussed in detail in Chapter Three. At this juncture, legislative privacy concerns are outlined briefly.

When Congress passed the Freedom of Information Act in 1966, it recognized that the accumulation of personal information by government threatened personal privacy. Two exemptions to the FOIA specifically shield personal privacy interests in government information. Exemption 6, which covers medical, personnel and "related" records,⁷⁵ and Exemption 7, which covers criminal history records,⁷⁶ acknowledge expectations of privacy in varying degrees. When information requesters have challenged agencies that have denied access under these exemptions, courts have attempted to balance privacy interests with the public's interest in disclosure of such information. However, the Supreme Court in Department of Justice v. Reporters Committee for Freedom of the Press has greatly narrowed what

constitutes a public interest in disclosure.⁷⁷ The ramifications of the 1989 opinion in Reporters Committee are discussed in Chapter Four.

Other exemptions also recognize privacy-like interests in business-related information held by government. Exemption 4 shields from disclosure confidential business information that agencies collect pursuant to their statutory duties.⁷⁸ Similarly, Exemption 8 protects certain banking records⁷⁹ and Exemption 9 protects valuable geological and geophysical information about oil and gas wells.⁸⁰

Lastly, Exemption 3 covers information declared confidential by other statutes.⁸¹ Several agencies have attempted to apply this exemption to the Privacy Act of 1974 as grounds for withholding information.⁸² These attempts prompted Congress to pass legislation specifically excluding the Privacy Act from Exemption 3 status.⁸³

The threat of computers to personal privacy first caught the attention of Congress in the 1960s, when congressional subcommittees held hearings on the possible development of a National Data Center, or centralized computerized data bank to pool information from various federal agencies. Several hearings were held on the National Data Center proposal and related technology issues throughout the 1960s, as the federal bureaucracy ballooned with President Lyndon Johnson's Great Society social

programs and the Vietnam war effort.⁸⁴ Proponents of a National Data Center pointed out the need for efficiency and enhanced decision making in the burgeoning bureaucracy. Opponents saw a centralized computer system as a serious threat to personal privacy and alluded to George Orwell's "Big Brother."⁸⁵

At a hearing in 1966, Representative Frank Horton of New York suggested that the very size and inefficiency of the federal bureaucracy held certain advantages for citizens.

One of the most practical safeguards . . . of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography of years of life. Retrieval is impractical and often impossible. A central data bank completely removes this safeguard.⁸⁶

Concern about the threat of government computers expressed at various congressional hearings,⁸⁷ underscored by the abuses of the Nixon administration during the Watergate era, ultimately led to passage of the Privacy Act of 1974.⁸⁸ The act recognized privacy as a fundamental right protected by the Constitution and threatened by widespread collection and dissemination of personal information by federal agencies. The act also recognized the positive role of computer technology in efficient government but sought to balance those positive aspects with the potential for abuse.

Since passage of the Privacy Act, Congress has responded to the new information technologies by passing

numerous measures to regulate the collection, distribution, and access to personal information held by the government.⁸⁹ Most recently, Congress passed the Computer Matching and Privacy Act of 1988 to put limitations on federal agencies' ability to share personal information via computers.⁹⁰

A Right of Access to Government Information

When the Founding Fathers gathered in Philadelphia more than 200 years ago to sort out differences endangering the tenuous union, they met in private. With an agenda that included potentially divisive issues, the Founders apparently believed secrecy more accommodating to the needs of the infant nation than the rigors of public debate. Self-preservation seemed paramount.⁹¹

Yet, this seemingly inauspicious beginning for a theory of access to the public's business belies the sentiments expressed in numerous writings by those instrumental in the American Revolution and by those who steadied the nation as it took its first unsure steps. A recurring theme was that the government served the people, that it existed only with the knowledge and consent of those governed. As James Madison, a dominant force behind the Bill of Rights, noted, "If we avert to the nature of Republic Government, we shall find that the censorial power is in the people over government, and not in the Government over people."⁹² From writings such as Madison's evolved a theory of democratic self-governance by an informed electorate, with a free and

vigorous press as a fundamental instrument in that process. This section looks at the development of the principle that the government's business is the people's business and that, as a result, the people have a fundamental right of access to that process and to information and records related to it. It explores the philosophical principles that gave rise to the values of free expression and a free press that influenced the Founding Fathers and how those values helped mold the new nation. It also traces the growth of values supporting access to government information that is integral to the contemporary concept of a self-governing society. In addition, the section looks at how the courts have viewed a right of access from a constitutional perspective and at how access has been incorporated into positive law through the legislative process.

Toward a Theory of Self-Governance

The free speech and free press clauses of the First Amendment to the U.S. Constitution and the concept of a well-informed, self-governing society grew from seeds planted more than a century before by English social and political philosophers. These philosophers wrote of the need to write and speak without government interference, of the importance of such freedoms within a society. These seeds would put down roots before and during the American Revolution and would flourish in the words of the Founding

Fathers, even if their actions sometimes seemed inconsistent with their words.⁹³

Libertarian Underpinnings

By most accounts, the genesis of libertarian thought was in the English poet John Milton's essay Aeropagitica in 1644, with its ritualistically quoted passage: "Give me liberty to know, to utter, and to argue freely according to conscience, above all liberties."⁹⁴ In Aeropagitica, Milton railed against government attempts to suppress his earlier writings that called for changes in the divorce laws that locked him in an unwanted marriage. Milton argued that government licensing of printers impeded the free flow of information and ideas, a process essential to the betterment of life and society. Milton said that people were capable of judging ideas and information for what they were worth, that in the process of sorting the good from the bad, truth would prevail. Said Milton, "And though all the winds of doctrine were let loose to play upon the earth, so Truth be in the field . . . Let her and Falsehood grapple; who ever knew Truth put to the worse, in a free and open encounter."⁹⁵ Rivaling Milton as a philosophical influence on the libertarian sentiments of the Founding Fathers' generation was John Locke, who maintained that governments have a duty to protect certain fundamental rights of citizens, such as life, liberty, and property. Compared to Milton, Locke held a radically different concept of the role of truth in public

discourse. While Milton focused on the tyranny and futility of suppression and in the belief that truth ultimately would triumph, Locke viewed truth as essentially unknowable.⁹⁶ He said people should be skeptical of their own opinions since they could never know for certain whether they were correct. Since knowledge was so frail and truth unknowable, Locke argued, it would be best to put all ideas before the public. Said Locke,

We should do well to commiserate our mutual ignorance, and endeavor to remove it in all the gentle and fair ways of information, and not instantly treat others ill or obstinate and perverse because they will not renounce their own and receive our opinions, or at least those we would force upon them, when it is more probable that we are no less obstinate in not embracing some of theirs. For where is the man that has uncontested evidence of the truth of all that he holds, or of the falsehood of all he condemns; or can say, that he examined to the bottom all of his own and other men's opinions?⁹⁷

Locke also argued that individuals enter society freely and as a matter of choice. Consequently, the government may exercise control over individuals only with their consent. All power to make laws resides with the citizenry, and only through the delegation of that power to the state may the state act.⁹⁸

Later essays of Englishmen John Trenchard and Thomas Gordon, writing under the pseudonym "Cato," also were a significant force behind the propagation of libertarian thought in colonial America. The essays were reprinted

widely in the colonial press and were popular reading. Said Cato,

That men ought to speak well of their Governors, is true, while their Governors deserve to be well spoken of; but to do public Mischief, without hearing of it, is only the Prerogative of Felicity and Tyranny; A free People will be shewing that they are so, by the freedom of speech.⁹⁹

Building on the Revolutionary Experience

The words of Milton, Locke, and Cato resonated through the colonists' revolutionary rhetoric as they became increasingly alienated under British rule. Locke's notion of the fundamental rights of individuals rings out in the Declaration of Independence, and the values of life, liberty and property pervade the Bill of Rights. The belief that free speech and a free press served as an essential check on the powers of government also found eloquent expression in the writings of those who shaped the new democracy.

Thomas Paine, whose Common Sense on the eve of the American Revolution helped draw waffling patriots into the revolutionary fold, expounded on the benefits of a representative democracy and the need for a full public accounting of government actions. Paine later wrote,

In the representative system, the reason for everything must publicly appear. Every man is a proprietor in government, and considers it a necessary part of his business to understand. It concerns his interest because it affects his property. He examines the costs, and compares it with the advantages; and above all, he does not adopt the slavish custom of following what in other governments are called leaders.¹⁰⁰

James Madison, the major proponent of the Bill of Rights, amplified the virtue of an informed society. Although writing about the role of information in the context of education, his premise suggests a parallel lesson for democratic society in general. He cautioned, "A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy, or perhaps both."¹⁰¹

Thomas Jefferson, writing in 1823, years after the tumult of the Revolution and the stressful period immediately following, cast himself "into the ranks of the most advanced libertarians . . . [with] his final testament on freedom of the press--a reflex of the best Enlightenment theory."¹⁰² Drawing on his own experience and observations, and on the collective wisdom of the libertarian philosophers, Jefferson described the press as a conveyor of information about the workings of government and as a stabilizing force in the rough-and-tumble of democratic society:

This formidable censor of the public functionaries, by arraigning them at the tribunal of public opinion, produces reform peaceably, which must otherwise be done by revolution. It is also the best instrument for enlightening the mind of man, and improving him as a rational, moral being.¹⁰³

Interestingly, even as Jefferson saw a free and vigorous press as a cornerstone of democracy, he did not view the press as free from "liability for personal

injuries." And at one point, not long after the expiration of the controversial Sedition Act in 1801, he suggested that the states should keep an unruly "Tory" press in check. Writing to Governor Thomas McKean of Pennsylvania, Jefferson opined that state restraints on the press might have a "wholesome effect in restoring the integrity of the presses . . . [and would] place the whole band more on their guard."¹⁰⁴

During the century that followed the American Revolution, when free speech and free press rhetoric flourished and strengthened the values underlying the First Amendment, another influential political philosopher would add to the theory that truth must have its day. John Stuart Mill acknowledged the value of free expression advanced by the earlier libertarian philosophers but discounted the argument that truth, given an opportunity, would always prevail. Mill, an ardent critic of American slavery, noted that truth frequently was suppressed and that its only chance to succeed lay in the right of free expression.¹⁰⁵ Mill also wrote about the concepts underlying a democratic society. Of the role of the individual in representative government, he suggested that government derives its authority from the governed; no democratic government would succeed without citizens willing to abide by certain rules and to do what was necessary to preserve it.¹⁰⁶ The foundation for such a society, Mill argued, was the

existence of powerful ideas and the ability of the majority to persuade others of their correctness.¹⁰⁷

Twentieth Century Legal Theory

The principles of the early libertarians and the words of the Founding Fathers and others regarding free expression and a free press lay the foundation for twentieth century legal theory and social philosophy supporting the role of a free and vigorous press in American society and its need for public information. Woodrow Wilson, in the first year of his presidency in 1913, eloquently expressed the sentiments of the nation's founders that government prospered only with the knowledge and consent of the people:

Whenever any public business is transacted, wherever plans affecting the public are laid, or enterprises touching the public welfare, comfort or convenience go forward, wherever political programs are formulated, or candidates agreed on, over that place a voice must speak, with the divine prerogative of a people's will, the words: "Let there be light."¹⁰⁸

The twentieth century concept of free expression was brought into focus in the second decade of the new century as it faced a severe test at a time when fears of social revolution dominated the legal and political establishments.

In 1919, amid the post-World War I social and political tumult in the United States over the Bolshevik revolution in Russia, U.S. Supreme Court Justice Oliver Wendell Holmes carried Milton's notion of free speech into the twentieth century discourse through the American free enterprise metaphor of the marketplace. The occasion was

the Supreme Court's opinion in Abrams v. United States, which upheld criminal convictions under the newly enacted Espionage Act.¹⁰⁹ The defendants were convicted of distributing materials critical of the United States' war effort that encouraged "disaffection, sedition, riots, and even revolution."¹¹⁰ The offending pamphlets, tossed from windows to passers-by, criticized the United States' decision to send troops to aid the czar during the revolution. In a dissenting opinion, Holmes took up the libertarian standard of free expression to reject the majority reasoning upholding the convictions based on words, not deeds. He argued for "free trade in ideas," even those we "loathe and believe to be fraught with death." Holmes said the "best test of truth is the power of the thought to get itself accepted in the competition of the market."¹¹¹ Holmes' notion of "the free trade of ideas" was often quoted by legal and political scholars when free speech was in question, and the importance of a free press in the marketplace of ideas became a rallying cry in the First Amendment lexicon.

In 1927, Justice Louis Brandeis, a dominant judicial force behind the notion of a fundamental right of privacy, argued with equal force for unfettered free expression limited only by the need "to protect the state" from "clear and imminent danger."¹¹²

In a concurring opinion in Whitney v. California, Justice Brandeis denounced a California syndicalism law as a threat to the fundamental principles of an informed, self-governing democracy, on which the nation was founded. He noted,

Those who won our independence believed that the final end of the state was to make men free to develop their faculties, and that in its government the deliberative forces should prevail over the arbitrary. They value liberty as both an end and as a means. . . . They believed that freedom to think as you will and to speak as you think are indispensable to the discovery and spread of political truth . . . that public discussion is a political duty; and that this should be a fundamental principle of the American government. . . . Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law--the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly would be guaranteed.¹¹³

The majority of the Court soon amplified this theme. In the 1931 case Stromberg v. California, the Court said that the First Amendment ensured "the opportunity for free political discussion to the end that government may be responsive to the will of the people and that changes may be obtained by lawful means."¹¹⁴ The role of a free press in the process of democratic self-governance was best articulated by Alexander Meiklejohn. Writing some 300 years after John Locke, Meiklejohn rejected the idea that freedom of speech derived solely from the natural law or rules of reason espoused by the Enlightenment philosophers. Rather, the venerable scholar anchored his theory of free expression

in the very nature of a self-governing democracy. Meiklejohn reasoned that the "principle of free speech springs from the necessity of the program of self-government. . . . It is a deduction from the basic American agreement that public issues shall be decided by universal suffrage."¹¹⁵ He said the First Amendment's protections for the practice of self-government are to ensure that the public retains control over government in the process of self-governance. He would have afforded absolute protection for expression about issues of self-governance because, he said, citizens need to gather and share information and opinions about their government to participate intelligently in the democratic process.¹¹⁶

Legal scholar Thomas Emerson couched Locke's principles of natural rights in the modern theory of self-actualization. The theory of self-actualization established an ascending hierarchy of essential needs to individuals in society. At the bottom were basic physical needs, such as food and shelter; at the top were the psychological needs of individuals to realize their full potential--or to be self-actualized.¹¹⁷ Emerson saw free speech and expression as essential to attainment of these higher needs. To Emerson, free expression was the embodiment of "the widely accepted premise of Western thought that the proper end of man is the realization of his own character and potentialities as a human being."¹¹⁸

Legal scholar Vincent Blasi offers another rationale for a strong, free press in American society. Echoing the sentiments of Paine and Jefferson that a free press as a "formidable censor of public functionaries" was essential to a democracy, he contends that a strong, free press is the most effective--if not the only effective--check on the potential abuse of power by government. Blasi accepts both Locke's argument for free expression based on fundamental rights and Meiklejohn's theory of self-governance. But he also casts the press--particularly the large, influential press--in another essential role as the only viable check on the equally powerful government.¹¹⁹

Blasi's arguments reflect those espoused by former Supreme Court Justice Potter Stewart, who saw in the First Amendment a "structural provision" giving the press rights separate and distinct from those of free speech. In a 1970 address at Yale Law School titled "Of the Press," Stewart rejected the view that the press should be only a neutral forum in the "marketplace of ideas." The press was not merely a vehicle for the balanced discussion of diverse ideas, he said. "Instead, the free press meant organized, expert scrutiny of government," Stewart said.¹²⁰ Implicit in both Meiklejohn's First Amendment theory of self-governance and Blasi's theory of the press as a fundamental check on government excess is the need for public and media access to the information government uses in decision making.

While freedom of the press and the implied importance of access to information have found solid support in the American experience, the legal parameters of press freedoms and a right of access have been shaped by legislatures and the courts. This development occurred at three levels. The first is the common law, where the notion of access to public information evolved through the daily application of laws and customs to resolve disputes and issues. The second is constitutional law. Constitutional analysis was triggered when the press asserted First Amendment rights to keep the public informed about the business of government. The third is statutory law, or positive laws enacted by legislatures recognizing varying degrees of a right of access.

A Common Law Right of Access

A legal concept of public access to government information developed within the common law. This concept initially was based on the personal interests of individuals in specific information, not on the premise that the public had a general right to inspect public records. Usually, access under the common law involved records sought during litigation. A Kentucky court summed up the early status of common law access:

[T]here is no common law right in all persons to inspect public documents or records; and that right, if it exists, depends entirely on the statutory grant. But . . . every person is entitled [to inspect public records] . . . provided he has an interest therein which is such

as would enable him to maintain or defend any action for which the document or record sought can furnish evidence of necessary information.¹²¹

Eventually, however, some courts began to expand the kinds of interest that would warrant access to public information. In 1903, for example, the state of Tennessee recognized a general taxpayers' interest in records concerning the financial condition of city government.¹²² In some jurisdictions, courts have abandoned entirely interest tests for access to public records.¹²³ Despite the willingness of some jurisdictions to recognize a broad-based public right under the common law, the most effective tools for access continue to be statutory. The statutory dimensions of public access will be discussed in a later section of this chapter.

Access and the Constitution

Acknowledging the important role of the press as primary sources of information in a self-governing society, the Supreme Court has recognized the constitutional right of the press to publish information it gathers about public issues.¹²⁴ But the Court has not articulated a First Amendment right of the press to obtain information that the government gathers, creates, or possesses outside the limited area of court proceedings. One jurist has likened the press without a right to gather and publish news to a "river without water."¹²⁵

This section looks at how the Supreme Court has viewed the right of the media to gather and publish news from a First Amendment perspective and at the implications various cases have for the flow of information in a self-governing society.

Before 1925, the First Amendment had functioned only as a limitation on actions of the federal government. But in that year, the Supreme Court first applied the First Amendment to actions of a state in a case that upheld a conviction based on the distribution of revolutionary literature. In Gitlow v. New York, the Court said that First Amendment rights protected from abridgment by Congress were "among the fundamental personal rights and 'liberties' protected by the due process clause of the Fourteenth Amendment from impairment by the states."¹²⁶ This selective application of certain parts of the Bill of Rights to the states through the Fourteenth Amendment is known as incorporation.¹²⁷

Since Gitlow, numerous cases have applied the First Amendment to affirm the roles of free speech and a free press in American society. For example, in 1931, the Supreme Court issued a landmark opinion in Near v. Minnesota that held prior restraints against the press were impermissible in all but the most extreme of circumstances.¹²⁸ More important to the development of a theory of access, however, are cases in which the Supreme

Court has addressed the rights of individuals to receive information and the rights of the public and the press to have access to government proceedings and information held by the government.

A right of the public to know about the workings of government, as such, is not stated in the U.S. Constitution. But the framers of the Constitution did include provisions for making government accountable to the people. The Constitution, in general terms, requires the legislative and executive branches of government to report regularly about their activities. Both Houses of Congress must keep and publish a "journal of its proceedings"¹²⁹ but may decide for themselves what might "require secrecy" and be withheld.¹³⁰ Congress also is required to "publish from time to time . . . a regular Statement and Account of the Receipts and Expenditures of all public Money."¹³¹ Similarly, the president is required to report to Congress "Information of the State of the Union."¹³² While these requirements for government accountability seem limited by modern access standards, they, nonetheless, reflected the fundamental principle that government should not function in secret or withhold information without good cause. Indeed, the fact the Constitution gives Congress the authority to determine what might "require secrecy" presupposes secrecy is the exception rather than the rule. Too, the limited expression of openness in the Constitution perhaps reflected

the realities of communications during the nation's formative years. The movement of information, even urgent information, was measured in terms of weeks and sometimes months; in times of war, battles were sometimes fought before word of an armistice could reach the battlefield.

The Right to Receive Information

The Supreme Court has never recognized a constitutional right of access to government information, or a right to gather information, on a par with the right to publish without prior government interference. The press may publish what it gathers, but government has no affirmative duty to facilitate the newsgathering process. The Court, however, has been more receptive to the rights of the public to receive information.

The Supreme Court has specifically recognized the rights of individuals to receive information in several cases. Perhaps, the first is Grosjean v. American Press Co., a 1936 case involving a challenge to a state tax that affected only large-circulation publications. A unanimous court struck down the tax as a violation of the First Amendment. The Court said a free press is a vital source of information and that "informed public opinion is the most potent of all restraints upon misgovernment."¹³³ The Court said First Amendment freedoms went "to the heart of the natural right of the members of an organized society, united in their common good, to impart and acquire information

about their common interests."¹³⁴ The Court concluded that the Louisiana tax would "limit the circulation of information to which the public is entitled by virtue of constitutional guarantees."¹³⁵

In 1969, the Supreme Court again recognized the public's right to receive information. In a broadcast regulation case involving the Federal Communications Commission's Fairness Doctrine, Red Lion Broadcasting Co. v. FCC, the Court held that broadcasters, who operated under a government license, may be compelled to grant individuals the right to reply on the air to political editorials and personal attacks. The Court recognized that government-regulated broadcasters had First Amendment rights but concluded that, on balance, the First Amendment rights of broadcast audiences to receive information were paramount. Interestingly, the court reasoned that broadcasters, by virtue of their license relationship with the government, had an affirmative duty to facilitate public access to information and ideas--a concept the Court has never imposed on government itself.¹³⁶ Neither has the Court imposed on the print media an affirmative duty to provide access to different points of view.¹³⁷

The Court also recognized the public's First Amendment right to receive information--even commercial information--in Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.¹³⁸ The Court struck down a state

statute barring pharmacists from advertising prescription drug prices. The Court's opinion focused on the public's strong interest in access to commercial information.¹³⁹ Such information, the Court reasoned, was essential if citizens were to make thoughtful consumer choices that, in the aggregate, could affect political issues such as the allocation of resources. "To this end, the free flow of commercial information is indispensable," the opinion stated.¹⁴⁰

The Court applied the First Amendment to the receipt of political information in First National Bank v. Bellotti, when it struck down a state law forbidding political advocacy by corporations. The Court reasoned that the public's right to receive political information is not diminished by the corporate identity of the speaker. The Court said the First Amendment's role was not only to foster individual expression but also to afford "the public access to discussion, debate, and the dissemination of information and ideas."¹⁴¹ The Court rejected the argument that "the relative voice of corporations" might drown out other less powerful speakers on controversial public issues. Instead, the Court said that in a democracy the public must choose among messages, whether the speaker be weak or strong.¹⁴²

A Right of Access to Government Information

While the Court has recognized the right of individuals to receive information from willing speakers, the question

of the public's and the media's constitutional right of access to government-held information is more problematic. Some cases, however, have implied at least a limited right of access to government functions and records. In Branzburg v. Hayes, the Court acknowledged that "without some protection for seeking out the news, freedom of the press could be eviscerated."¹⁴³ But on a 5-4 vote, the Court rejected a special privilege for news reporters not to have to testify before grand juries. In Branzburg, three journalists argued that if they were forced to reveal names of confidential sources, to whom they had pledged confidentiality, news organizations would lose their credibility. Too, sources would cease to come forward, and society might be deprived of important information, they said. Justice Powell, who joined the majority opinion as the key fifth vote, stated in a concurring opinion that any claim of press privilege should be weighed on a case-by-case basis, thus recognizing at least the possibility that in some circumstances the press might warrant special consideration.¹⁴⁴ Powell's reasoning, when combined with the rationale of the dissenting justices, led many appellate courts during the 1980s to recognize a limited First Amendment newsgathering right for journalists with respect to protecting confidential sources, at least in cases not involving grand juries.¹⁴⁵

In a pair of cases dealing with access to prisoners and prisons, the Court has said the press had no greater right of access to government information than any other members of the public. In Pell v. Procunier¹⁴⁶ and Saxbe v. Washington Post Co.,¹⁴⁷ cases heard jointly, the Court upheld federal regulations restricting press interviews with prisoners. Important to the Court's analysis, however, was that access to prisons was traditionally restricted and therefore the media were not being singled out. Writing for the majority, Justice Stewart said the press was free to gather what it can and to publish what it knows. But, Stewart said,

This autonomy cuts both ways. The press is free to do battle against secrecy and deception in government. But the press cannot expect from the Constitution any guarantee that it will succeed. There is no constitutional right to have access to particular government information, or to require openness from the bureaucracy.¹⁴⁸

In Pell and Saxbe, Justice Douglas, writing for the three dissenters, argued that the press should have a right of access greater than the public generally. He said the press, as a vehicle for the transmission of ideas and information, held a "preferred position in our constitutional scheme" and that the public's "right to know is crucial to the governing powers of the people."¹⁴⁹

While the Supreme Court has said the public and media have no right of access to prisons, it has held that the First Amendment requires criminal trials to be open. In

Richmond Newspapers v. Virginia, the Court said criminal trials "must be open to the public" absent an overriding competing interest, even when a defendant wanted the trial closed.¹⁵⁰ In a plurality opinion, Chief Justice Burger engaged in a historical as well as a First Amendment analysis. He noted that trials in England and in this country had historically been public affairs. The chief justice cited English customs dating to before the Norman Conquest that gave rise to the jury system. When cases were brought before courts, freemen of the community were required to attend and render a judgment. In reasoning that could apply equally to access to all forms of government proceedings, he noted,

This is no quirk of history; rather, it has long been recognized as an indispensable attribute of the Anglo-American trial. . . . It gave assurances that the proceedings were conducted fairly to all concerned, and it discouraged perjury, the misconduct of participants, and decisions based on secret bias or partiality.¹⁵¹

He also noted the therapeutic value of open proceedings and the importance of such openness in ensuring confidence in the process of government. "People sensed from experience and observation that, especially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and the results."¹⁵² The chief justice echoed Thomas Jefferson's notion that exposing government actions in the "tribunal of public opinion"

diffused emotions and led to peaceable reforms. He observed that openness provided an "outlet for community concern, hostility, and emotion," and that without knowledge the system was working, "natural human reactions of outrage and protest are frustrated and may manifest themselves in some form of vengeful 'self-help,' as indeed they did regularly in the activities of vigilante 'committees' on the frontiers."¹⁵³ He pointed out that people do not demand infallibility from their institutions, but that "it is difficult for them to accept what they are prohibited from observing."¹⁵⁴

After outlining the need for openness in government--at least in court proceedings--the chief justice turned his attention directly to the special role of the press as a surrogate for the people. He noted that while the First Amendment right to assemble in public places and to attend trials covers the public generally, the press acts as a stand-in for the public; therefore, without press access, public access is diminished.

It is not crucial whether we describe this right to attend criminal trials to hear, see, and communicate observations concerning them as a "right of access," or a "right to gather information," for we have recognized that "without some protection for seeking out the news, freedom of the press could be eviscerated." The explicit, guaranteed rights to speak and publish concerning what takes place at a trial would lose much meaning if access to observe the trial could, as it was here, be foreclosed arbitrarily.¹⁵⁵

Chief Justice Burger also made quick work of the argument that there was no right of public access to court proceedings because no such right was spelled out in the Constitution. He pointed out that during the debate over whether the Constitution should have a Bill of Rights, it was made clear that just because the Constitution did not grant a particular right, this did not mean no such right existed. In words that could bolster an argument for an implicit First Amendment right of access to government information modeled along the lines of reasoning supporting a constitutional right of privacy, he noted,

Notwithstanding the appropriate caution against reading into the Constitution rights not explicitly defined, the Court has acknowledged that certain unarticulated rights are implicit in enumerated guarantees. For example, rights of association and of privacy, the right to be presumed innocent and the right to be judged by a standard of proof beyond a reasonable doubt in a criminal trial, as well as the right to travel, appear nowhere in the Constitution or Bill of Rights. Yet these important but unarticulated rights have nonetheless been found to share constitutional protection in common with explicit guarantees . . . fundamental rights, even though not expressly guaranteed, have been recognized by the Court as indispensable to the enjoyment of rights specifically defined.¹⁵⁶

Justice William Brennan, author of the Court's landmark 1964 libel opinion in New York Times v. Sullivan, concurred with the result in Richmond but focused on the "structural role" the media play in the American system of self-government. Alluding to Alexander Meiklejohn's theory of democratic self-governance, Justice Brennan reasoned that

the First Amendment was meant to do more than protect free communication for its own sake. Rather, he said,

Implicit in this structural role is not only "the principle that debate on public issues should be uninhibited, robust and wide-open," but the antecedent assumption that valuable public debate--as well as other civic behavior--must be informed. The structural model links the First Amendment to that process of communication necessary for a democracy to survive, and thus entails solicitude not only for communication itself, but for the indispensable conditions of meaningful communication.¹⁵⁷

For communication to be meaningful in a self-governing society, Justice Brennan concluded, public and press access to government information are essential. In words that anticipated his approach to the access/privacy conflict that would arise over the government's growing use of computers, he said, "Our decisions must therefore be understood as holding only that any privilege of access to governmental information is subject to a degree of restraint dictated by the nature of the information and countervailing interests in security and confidentiality."¹⁵⁸ (Emphasis added.)

In a separate concurring opinion, Justice Stevens termed Richmond "a watershed case" and suggested that "for the first time the court unequivocally holds that an arbitrary interference with access to important information is an abridgment of the freedom of speech and of the press."¹⁵⁹ In the wake of Richmond, some legal scholars shared Justice Stevens' position, suggesting that the opinion cast the First Amendment as a sword with which to

"secure information from a reluctant government."¹⁶⁰ While increased access has occurred in other trial-related areas,¹⁶¹ pronouncements that Richmond was "a watershed case," signaling a significant shift in access doctrine proved exaggerated.¹⁶²

Statutory Access to Government Information

If the Supreme Court has been reluctant to recognize a First Amendment right of access to government information beyond the courts, Congress has been willing to enact legislation opening federal regulatory agencies to public scrutiny. But statutory recognition of a public right of access to government information is a relatively new phenomenon that developed in the two decades following World War II.

In 1946, Congress enacted the Administrative Procedures Act,¹⁶³ which recognized the public character of government records gathered and kept by federal executive agencies. But the act's inexact language, which allowed agencies to determine what information "requiring secrecy in the public interest" should be exempt from disclosure, provided a loophole that led to widespread, arbitrary withholding. The act, in effect, became more of a withholding statute. During this post-World War II period, proponents of access to government information were given a boost when the government issued the Hoover Study Report, which led to passage of the Federal Records Act of 1950.¹⁶⁴

As the 1950s unfolded, press organizations and other advocates of open government began a push to open up federal executive agencies, which had increased the level of secrecy as the Cold War and the threat of communism took hold. In one effort to promote access, the American Society of Newspaper Editors commissioned a report on the customs, law, and legislation dealing with access to government information. The result was The People's Right to Know, a book promoting access by media lawyer Harold Cross.¹⁶⁵ Cross began the seminal study about access to government information with this statement:

Public business is the public's business. The people have a right to know. Freedom of information is their just heritage. Without that citizens of a democracy have but changed their kings. . . . Citizens of a self-governing society must have the legal right to examine and investigate the conduct of affairs, subject only to those limitations imposed by the most urgent public necessity.¹⁶⁶

Cross concluded that the solution to the problem of access to government information lay with the legislative process:

Congress is the primary source of relief. . . . The time is ripe for an end to ineffectual sputtering about executive refusals of access to official records and for Congress to begin exercising its function to regulate freedom of information for itself, the public and the press.¹⁶⁷

Despite Cross' call on Congress for relief, the "ineffectual sputtering" would continue for a while. Shifting of political fortunes, however, would soon provide

an important nudge. In 1955, President Dwight Eisenhower was elected to a second term. But while the Republican won the White House, the majority in the House of Representatives swung to the Democrats, and along with majority-party status came committee chairmanships. Congress had become increasingly concerned about its inability to pry information from Republican-controlled executive agencies. Various committees, now under Democratic leadership, provided forums for a public access debate.¹⁶⁸

In 1955, California Congressman John Moss began hearings on the access issue that would continue for some 10 years. The work of the Moss Committee, along with that of other access advocates such as Cross and Ralph Nader,¹⁶⁹ culminated in 1966 with passage of the federal Freedom of Information Act. When President Lyndon Johnson signed the legislation, he observed that "a democracy works best when the people have all the information that the security of the nation permits."¹⁷⁰ The purpose of the act, according to the Senate report on the legislation, was to close loopholes in the Administrative Procedures Act and to foster "a general philosophy of full agency disclosure."¹⁷¹ The Supreme Court later put its imprimatur on this goal in an FOIA-related opinion. "The basic purpose of the FOIA is to ensure an informed citizenry, vital to the functioning of a democratic

society, needed to check against corruption and to hold the governors accountable to the governed," the Court stated.¹⁷²

Under the FOIA, all agency records must be disclosed unless specifically exempted. The act places the burden on the agency to justify withholding. While the FOIA's purpose is "full agency disclosure," it also contained nine exemptions that recognized competing social values.¹⁷³ Several of these exemptions, discussed in a previous section, specifically attempt to balance the public's right to know with the privacy interests of individuals on whom the government keeps information.

In addition to access to records, Congress also has passed "Government in the Sunshine" legislation requiring some 50 federal agencies, boards, and commissions to open most of their meetings to the public.¹⁷⁴

State Access to Government Records

Legislative recognition of a public right of access to information is not limited to the federal government. Before 1940, only 12 states had substantial public access statutes.¹⁷⁵ By 1992, all 50 states and the District of Columbia recognized the public's right of access to government records.¹⁷⁶ The state statutes vary in the degree of openness allowed and the definition of public records. Some provide access to a narrow range of records, such as records required to be kept by state law; others take a sweeping view of access, opening all records pertaining to

any aspect of state business. Perhaps, the preamble to the Indiana Open Records Law best sums up the thrust of most state access legislation:

A fundamental philosophy of the American constitutional form of representative government is that government is the servant of the people and not their master. Accordingly, it is the public policy of that state that all persons are entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees.¹⁷⁷

Privacy and Access in Conflict

The foregoing discussion of the values supporting a right of privacy and values supporting public access to government information suggest both are well-grounded in the American experience.

Where core privacy values have been involved, such as those involving unlawful searches, intimate personal decisions, or freedom of association, the Supreme Court has demanded government show a compelling interest before infringing on those values. In informational privacy cases, the Court also has imposed constitutional limitations on government. At the very least, the Court has recognized that when government gathers and stores personal information about individuals, it has a concomitant duty to ensure the privacy of that information. When private information is held in government computers, the Court requires government place a high priority on the security of such information systems. Exactly how privacy is defined remains a problem.

In legislation, Congress also has clearly recognized the privacy rights of individuals who relinquish personal information to the government, most prominently the Privacy Act of 1974. A major factor in the Privacy Act and much subsequent legislation resulted from concerns about the threat of computers to personal privacy.

While privacy is a core societal value, the right of the public and the press to government information, likewise, is at the core of the process of democratic self-governance. Although the Supreme Court has held that a general right of access lacks the constitutional dimension of the right of privacy, the values underlying the public's right to know about government are no less fundamental and are deeply embedded in the American experience. The value of an informed electorate is rooted in the nation's drive to independence and has been articulated in many ways during more than two centuries. The legitimate role of access to information has been recognized as a core social value by Congress, which in a democratic society reflects the will of the people.

These important values at times conflict, as the public and press seek information, sometimes containing private data, about how government goes about the people's business. At times, one right or the other must yield in the interest of society. Chapter Three will look at how Congress and the courts have attempted to balance these interests, at a time

when the center of balance has been skewed by concerns about the widespread use of government computers to gather and store information about individuals. The chapter will track the development of congressional concerns about the threat of computers to personal privacy, focusing on hearings leading up to passage of the Privacy Act of 1974.

Notes

1. See Harold Cross, The People's Right to Know xiv (1953). "Public business is the public's business. The people have a right to know. Freedom of information is their just heritage. Without that citizens of a democracy have but changed their kings. . . . Citizens of a self-governing society must have the legal right to examine and investigate the conduct of affairs, subject only to those limitations imposed by the most urgent public necessity."
2. Olmstead v. United States, 227 U. S. 438, 478 (1928). U.S. Supreme Court Justice Louis Brandeis wrote: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, as against the Government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized man."
3. Florida Star v. B.J.G., 109 S.Ct. 2603, 2609 (1989).
4. Griswold v. Connecticut, 381 U.S. 479, 486 (1965), Justice Goldberg, joined by Chief Justice Warren and Justice Brennan, concurring.
5. Id. at 494.
6. Genesis 3:7, 3:21.
7. Richard F. Hixson, Privacy in a Public Society: Human Rights in Conflict 3 (1987).
8. Morris L. Ernst and Alan U. Schwartz, The Right To Be Let Alone 5-6 (1962).
9. Id.
10. John Locke, The Second Treatise on Government 55-81 (T. Peardon ed. 1952).

11. Griswold v. Connecticut, supra note 4.
12. David H. Flaherty, Privacy in Colonial New England 5 (1972).
13. Id. at 1.
14. Id. at 248.
15. Id. at 121.
16. Id. at 249. The Supreme Court later found a right of privacy in the "penumbra" of these amendments. Griswold v. Connecticut, supra note 4 at 484.
17. Hixson, Privacy in a Public Society at 13.
18. John H.F. Shattuck, Rights of Privacy 5 (1977).
19. Id. See U.S. Const. amend. IV. The Fourth Amendment states: The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
20. John Stuart Mill, On Liberty, quoted in William Cohen and John Kaplan, Constitutional Law: Civil Liberty and Individual Rights 532 (2d ed. 1982).
21. Demay v. Roberts, 46 Mich. 160, 9 N.W. 146 (1881).
22. Id. at 148.
23. Michael Emery and Edwin Emery, The Press in America: An Interpretive History of the Mass Media 188 (6th ed. 1988). See also Don R. Pember, Privacy and the Press 6-10 (1972).
24. Id. at 184, 186.
25. Alan F. Westin, Privacy and Freedom (1967).
26. Id. at 338.
27. "The Telephone Unmasked," The New York Times, October 12, 1877, at 4.
28. Id.

29. William Prosser, "Privacy," 48 Calif. L. Rev. 383-384 (1960). See also Pember, Privacy and the Press at 10-19.

30. Samuel D. Warren and Louis Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 195 (December 1890).

31. Id. at 220.

32. Some scholars play down the impact of the article by Warren and Brandeis. For example, one scholar argues that little consideration has been given to the concept of freedom of the press, described as an unimportant legal concept at the time. However, the scholar points out that in the twenty years after "The Right to Privacy" was published, many courts rejected the tort of privacy because it interfered with freedom of the press. See Pember, Privacy and the Press at 57. See also Harry Kalven, "Privacy and Tort Law--Were Warren and Brandeis Wrong?" 31 Law & Contemp. Probs., 326, 333 (1966).

33. Schuyler v. Curtis, 15 N.Y. Supp. 787, 788 (1891).

34. Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).

35. Id. at 442.

36. Id. Citing New York Civil Rights Law (McKinney) secs. 50-51 (1976).

37. Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

38. 1 Letters of Louis D. Brandeis 306 (M. Urofsky and D. Levy eds. 1971).

39. Westin, Privacy and Freedom at 338.

40. Prosser, "Privacy," supra note 29.

41. Restatement (Second) of Torts sec. 652D (1977).

42. Griswold v. Connecticut, supra note 4. While the U.S. Constitution does not specifically mention privacy, several state constitutions do. See Alaska Const. art I, sec 22; Ariz. Const. art. 2, sec. 8; Cal. Const. art I, sec. 1; Fla. Const. art I, sec. 23; Haw. Const. art I, sec 6; Ill. Const. art I, sec. 12; La. Const. art I, sec. 5; Mass Gen. Laws Ann. ch. 214, sec. 1(b); Mont. Const. art II, sec 10; S.C. Const. art. I, sec. 10; Wash. Const. art. I, sec. 7.

43. Boyd v. United States, 116 U.S. 616 (1886).
44. Id. at 630.
45. Westin, Privacy and Freedom at 67-157. See also Harry Kalven, Jr., "The Problems of Privacy in the Year 2000," 96 Daedalus 876-882 (Summer 1967).
46. Olmstead v. United States, 277 U.S. 438, 475-478 (1928).
47. Goldman v. United States, 316 U.S. 129, 138 (1942).
48. Mapp v. Ohio, 367 U.S. 644 (1961).
49. Id. at 660. The issue of unlawful search and seizure will be discussed later in the context of computer matching, or the cross-referencing of government data bases. Individuals usually give information to the government for a specific reason, such as receipt of certain benefits. The cross-referencing of data bases results in data collected for one reason being compared with data collected for other reasons, without the subject's knowledge. Such "searches" raise questions about legal due process.
50. NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).
51. Id. at 462.
52. Shelton V. Tucker, 364 U.S. 479 (1960).
53. See supra note 12.
54. Allgeyer v. Louisiana, 165 U.S. 578, 579 (1897).
55. Substantive due process, which struck down much worker-related protective legislation on the grounds of the economic "liberty" of workers and their freedom of contract, lost favor during the 1930s when the Supreme Court shifted in the face of Depression-era economic regulations. The Court began to uphold New Deal legislation that earlier had been struck down because it interfered with the rights of individuals to make economic decisions. The issues of substantive due process remained controversial into the 1990s in the context of the right-to-an-abortion debate; instead of economic liberty, however, the issue is "reproductive" liberty. See David A. Kaplan, "Is Roe Good Law? What's Wrong With the Historic Decision--And the Attacks Against It," Newsweek, April 27, 1992, at 49-51.

56. Allgeyer v. Louisiana at 579.
57. Meyer v. Nebraska, 262 U.S. 390 (1923).
58. Id. at 399.
59. Pierce v. Society of Sisters, 268 U.S. 510, 535 (1925).
60. Griswold v. Connecticut, supra note 4. See also David Dixon, "The Griswold Penumbra: Constitutional Charter for the Expanded Law of Privacy?" 64 Mich. L. Rev. 197, 199 (1965).
61. Id. at 485.
62. Id.
63. Id. at 500.
64. Id., citing Poe v. Ullman, 367 U.S. 497 (1961).
65. Roe v. Wade, 410 U.S. 113 (1973).
66. United States v. Miller 425 U.S. 435 (1976).
67. Id. at 451-52.
68. Whalen v. Roe, 429 U.S. 589 (1977).
69. Id. at 605.
70. Id.
71. Id. at 607.
72. United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).
73. Id. at 764.
74. Id. at 764. Citing Westin, Privacy and Freedom (1972) at 7. "Privacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."
75. Freedom of Information Act, 5 U.S.C. sec. 552(b) (6).
76. Id. at 5 U.S.C. sec. 552(b) (7).

77. Justice Department v. Reporters Committee for Freedom of the Press at 771.

78. Freedom of Information Act, 5 U.S.C. sec. 552(b) (4).

79. Id. at 5 U.S.C. sec. 552(b) (8).

80. Id. at 5 U.S.C. sec. 552(b) (9).

81. Id. at 5 U.S.C. sec. 552(b) (3).

82. See Thomas Susman, "The Privacy Act and Freedom of Information Act: Conflict and Resolution," 21 J. Marshall L. Rev. 703 (Summer 1988).

83. Congress cleared up the misunderstanding in 1984 with an amendment to the National Security Act of 1947 that specifically stated that the Privacy Act did not qualify as an Exemption 3 statute under the Freedom of Information Act. Pub. L. No. 99-145, amending 50 U.S.C.A. sec. 431.

84. See generally The Computer and Invasion of Privacy: Hearings Before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations, 89th Cong., 2d Sess. (1966); Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 92nd Cong., 1st Sess. (1971); Privacy: The Collection, Use and Computerization of Personal Data: Joint Hearings Before the Subcommittee on Privacy and Information Systems of the Senate Committee on Government Operations and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 93rd Cong., 2d Sess. (1974).

85. The Computer and Invasion of Privacy, supra note 84 at 13.

86. Id. at 6.

87. See supra note 84.

88. Privacy Act of 1974, 5 U.S.C. sec. 552a. See also S.Rep. No. 93-1183, reprinted in U.S. Cong. & Admin. News 6926 (1974).

89. Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. sec. 552a; Right to Financial Privacy Act of 1978, 12 U.S.C. sec. 3401; Electronic Communications Privacy Act of 1986, 18 U.S.C. sec. 2510; Computer Security Act of 1987, Pub. L. No. 100- 235; Federal Managers' Financial

Integrity Act of 1982, 31 U.S.C. sec. 3512; Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474; Cable Communication Policy Act of 1984, 47 U.S.C. sec. 521; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. sec. 1232.

90. Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. sec. 552a.

91. Westin, Privacy and Freedom at 334.

92. 4 Annals of Cong. 934 (1794).

93. For example, the constitutional convention excluded the public (see supra note 91), and Thomas Jefferson soon after expiration of the Sedition Act suggested in a letter to the governor of Pennsylvania that the states should act to control the "Tory" press (see Leonard Levy, Emergence of a Free Press 341 (1985). See Nat Hentoff, The First Freedom 86 (1980). See generally Leonard Levy, Jefferson and Civil Liberties: The Darker Side (1963).

94. Levy, Emergence of a Free Press at 93.

95. 1 The Prose Works of John Milton 198 (Rufus W. Griswold ed. 1856).

96. John Locke, IV An Essay Concerning Human Understanding 560-561 (1952), as noted in Levy, Emergence of a Free Press at 97.

97. Id.

98. Locke, The Second Treatise on Government at 55-81.

99. Levy, Emergence of a Free Press at 110. See also Emery and Emery, The Press in America: An Interpretive History of the Mass Media at 14.

100. Thomas Paine, The Rights of Man 38 (1984).

101. Letter from James Madison to W.T. Barry (Aug. 4, 1822), pertinent portion reprinted in The Complete Madison 337 (Saul K. Padover ed. 1953). Cited in Environmental Protection Agency v. Mink, 410 U.S. 73, 110-111 (1973).

102. Levy, Jefferson and Civil Liberties: The Darker Side at 69.

103. Id.

104. Letter from Thomas Jefferson to Gov. Thomas McKean of Pennsylvania (Feb. 19, 1803), reprinted in 9 The Writings of Thomas Jefferson 451-452 (Paul Leicester Ford ed. 1892-1899). Cited in Levy, Emergence of a Free Press at 341. See also Emergence of a Free Press at 250-281 for a discussion of Jefferson's belief in state prohibitions against the press.

105. See generally John Stuart Mill, On Liberty (1863).

106. John Stuart Mill, Considerations on Representative Government 6-9 (C. Shields ed. 1958).

107. Id. at 12-15.

108. Woodrow Wilson, The New Freedom 86 (1913).

109. Abrams v. United States, 250 U.S. 616 (1919).

110. Id. at 630.

111. Id. (Justice Holmes dissenting.)

112. Whitney v. California, 274 U.S. 357 (1927).

113. Id. at 375-376.

114. Stromberg v. California, 274 U.S. 359, 369 (1931).

115. Alexander Meiklejohn, Free Speech and Its Relation to Self-Government 89-94 (1948).

116. Id.

117. See generally Abraham Maslow, Motivation and Personality (1954), and Maslow, Religion, Values and Peak-Experience (1970).

118. Thomas Emerson, Toward a General Theory of the First Amendment 4-5 (1963). See also Emerson, The Bill of Rights Today (1973).

119. Vincent Blasi, "The Checking Value in First Amendment Theory," 1977 Am. B. Found. Res. J. 521, 538.

120. Potter Stewart, "Or of the Press," 26 Hastings L. J. 631, 633-36 (1975). See also Floyd Abrams, "The Press Is Different: Reflections on Justice Stewart and the Autonomous Press," 7 Hofstra L. Rev. 563 (1979).

121. Fayette Co. v. Martin, 279 Ky. 387, 396, S.W. 2d 838, 843 (1939).

122. State ex rel. Wellford v. Williams, 110 Tenn. 549, 75 S.W. 948 (1903). See also Clement v. Graham, 78 Vt. 290 (1906).

123. Burton v. Tuite, 78 Mich. 363 (1889); MacEwan v. Holm, 226 Or. 27 (1961).

124. See generally Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976); United States v. Nixon, 418 U.S. 683 (1974).

125. In re Mack, 368 Pa. 251, 273, A.2d 679, 689 (1956), cert. denied 352 U.S. 1002 (1957).

126. Gitlow v. New York, 268 U.S. 652 (1925).

127. Through a series of opinions, the U.S. Supreme Court extended provisions of the Bill of Rights to cover actions by the states. The Court incorporated the Bill of Rights into the Fourteenth Amendment by holding that state infringements on free speech and other rights deprive individuals of due process guaranteed by the Fourteenth Amendment.

128. Near v. Minnesota, 283 U.S. 697 (1931).

129. U.S. Const. art. I, sec. 5, cl. 3.

130. Id.

131. Id., art. I, sec. 9, cl. 7.

132. Id., art III, sec. 3.

133. Grosjean v. American Press Co., 297 U.S. 233 (1936).

134. Id. at 250.

135. Id. at 243.

136. Red Lion Broadcasting v. FCC, 395 U.S. 367 (1969).

137. Miami Herald v. Tornillo, 418 U.S. 241 (1974).

138. Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976).

139. Id. at 765.

140. Id. Justice Rehnquist dissented sharply from the majority, arguing that the opinion devalued the First Amendment. He said the First Amendment should protect the "marketplace of ideas," not the commercial marketplace. Id. at 781-790.

141. First National Bank v. Bellotti, 435 U.S. 765 (1978).

142. Id. at 789-790.

143. Branzburg v. Hayes, 408 U.S. 655, 681 (1972).

144. Id. at 710 (Justice Powell concurring).

145. Kent Middleton and Bill F. Chamberlin, The Law of Public Communication 488 (2d ed. 1988).

146. Pell v. Procunier, 417 U.S. 817 (1974).

147. Saxbe v. Washington Post Co., 417 U.S. 843 (1974).

148. Pell v. Procunier at 834.

149. Id. at 840 (Justice Douglas dissenting).

150. Richmond Newspapers v. Virginia, 448 U.S. 555 (1980).

151. Id. at 569.

152. Id. at 571.

153. Id.

154. Id. at 572.

155. Id. at 577.

156. Id. at 579.

157. Id. at 587-588.

158. Id. at 586.

159. Id. at 582.

160. William Van Alstyne, Interpretations of the First Amendment 54 (1984).

161. See e.g., Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979); Globe Newspaper Co. v. Superior Court, 457 U.S. 596 (1982); Press-Enterprise Co. v. Riverside County Superior Court, 464 U.S. 501 (1984).
162. Pell v. Procunier at 834.
163. Administrative Procedures Act, 5 U.S.C. sec. 1002 (1946).
164. Federal Records Act, 64 Stat 583 (1950).
165. See generally Cross, The People's Right to Know.
166. Id. at xxx.
167. Id. at xiv.
168. See Paul E. Kostyu, "Political Pressure: The Freedom of Information Act and John E. Moss Jr.," conference paper presented at the AEJMC Southeast Colloquium in Orlando, Fla. (Feb. 28-March 2, 1991).
169. See generally James R. Wiggins, Freedom or Secrecy? (1964); Ralph Nader, Unsafe at Any Speed: The Designed-in Danger of the American Automobile (1965).
170. Quoted in Thomas Susman, "Introduction to the Issues, Problems, and Relevant Law" in "Your Business, Your Trade Secrets, and Your Government," 34 Admin. L.R. 117 (1982).
171. S. Rep. No. 813, 89th Cong., 1st Sess. 3 (1965).
172. NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978). The Court said: "The basic purpose of the FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and hold the governors accountable to the governed."
173. Freedom of Information Act, 5 U.S.C. sec. 552(b) (1-9).
174. Id. at 5 U.S.C. sec. 552b(a).
175. See Reporters Committee for Freedom of the Press, Tapping Official Secrets: A State Open Government Compendium (1989).
176. See Comments, "Public Inspection of State and Municipal Executive Documents: Everybody, Practically

Everything, Anytime, Except . . ." 45 Fordham L.R. 1105, 1107 (1977).

177. Ind. Code sec. 5-14-3-1 (1977). See also Texas Stat. sec. 6252-17a. The Texas law states:

Pursuant to the fundamental philosophy of the American constitutional form of representative government which holds to the principle that government is the servant of the people, not the master of them, it is hereby declared to be the public policy . . . that all persons are, unless otherwise expressly provided by law, at all times entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may retain control over the instruments they have created.

CHAPTER THREE
THE EVOLUTION OF COMPUTER/PRIVACY CONCERNS:
ACCESS TO GOVERNMENT INFORMATION HELD IN THE BALANCE

The Core of the Debate

Concerns about threats to personal privacy have played a central role in laws and legislation placing limitations on public and media access to government information. Governments at all levels--federal, state and local--increasingly require individuals seeking benefits, services, and legal intervention to relinquish certain personal information. To deal with this vast accumulation of information, and to use it effectively to benefit society, governments have grown to rely more and more on computers.¹

For some three decades, realistic and sometimes exaggerated concerns about the role of computers in society have driven the public policy debate over personal privacy. The issue was first raised in the 1960s, when the federal Bureau of the Budget floated a proposal for a National Data Center in which to pool information from various government agencies. Congressional hearings over the controversial proposal provided a forum for worry over the potential dangers of computers and started a process that led to the

Privacy Act of 1974 and related privacy legislation. The public policy debate over the property bounds of personal privacy continued into the 1990s, with concerns about the computer at its core. The proper relation between personal privacy and public and media access to government information continues to be its focus.

The importance of that relationship was underscored by the U.S. Supreme Court in the 1989 case U.S. Department of Justice v. Reporters Committee for Freedom of the Press, which dealt with a media attempt to obtain information contained in a government data base. Among other things, that opinion concluded that the accumulation of personal information in centralized government computers--even when the information was taken from public records elsewhere--enjoyed a rejuvenated privacy interest when drawn into a centralized data base. The Reporters Committee opinion also concluded that such compilations of information could be categorically exempt from disclosure without undergoing the traditional case-by-case balancing of the privacy interests at stake with the public interest served by disclosure.² The congressional concern about privacy and computers runs wide and deep. While most legislative action has sought to place controls on how government gathers and uses information, such concerns for privacy have implications for public and media access. Laws written to ensure privacy--especially after fears about computers have been voiced--run

the risk of being overbroad, shielding more information than necessary from public access to achieve their policy aims. Too, privacy statutes that include criminal penalties incline record custodians to err on the side of withholding information when the requested information does not fit clearly into a nonexempt category.

This chapter tracks the development of legislative concerns about privacy and the role that fears about computers have played in those concerns. It focuses on development of the computer, its growing use in government, and on the conflict created between important social needs--for efficient government and for the privacy rights of people on whom government keeps files.

The chapter begins with an overview of social, political, and technological forces after World War II that led to concerns among social scientists, legal scholars, social commentators, and politicians about computers. To provide a context for this overview, the chapter briefly traces the shift of government from its limited role as protector of economic opportunity to that of active social planner and provider of social benefits.

The chapter also looks at other societal concerns contributing to the American milieu as questions about government use of information technology became a public issue--and a love-hate relationship with technology evolved.

Backdrop for the Computer/Privacy Debate

In the decade following World War II, the Cold War focused the attention of Americans on the threat of Soviet communism and, more generally, totalitarian government. George Orwell's popular postwar novel 1984, a fictional account of an omniscient totalitarian regime that trampled individual liberties, gave form to these anxieties in the person of "Big Brother."³ Senator Joseph McCarthy manipulated these fears for political advantage, and the U.S. Supreme Court upheld convictions of several communists during this time. Finally, developing computer technologies brought the nation, technologically at least, a step closer to 1984.

Emerging from World War II as the most prosperous and powerful nation in the world, the United States had as one of its immediate tasks the rebuilding of Europe as a bulwark against communism. The ideological standoff that ensued between the Soviet Union and the United States and its allies was exemplified in the mortar and brick of the Berlin Wall and Winston Churchill's metaphor of the Iron Curtain.⁴ The Cold War of the early 1950s, underscored by an undeclared war with communist North Korea under the auspices of the United Nations, was fertile ground for the likes of Joseph McCarthy. The senator from Wisconsin gained political capital by challenging the patriotism of many employees of the federal bureaucracy, quite a few New Deal

Democrats instrumental in the social legislation of the Great Depression era. With memories of Hitler still fresh, and the communist threat played out daily on the battlefields of Korea and in newspaper headlines, McCarthy for a time had his way with politicians, public, and press.⁵ The commandeering of government by subversives seemed a real danger, and McCarthy exploited such fears with unfounded accusations. The U.S. Supreme Court also reflected the anxieties of the times. The Court upheld the convictions of several communists whose crimes were advocacy of a despised ideology, not overt acts of insurrection.⁶ Indeed, the U.S. policy toward Indochina, based on fear of a "Domino Effect" in Southeast Asia should any nation there succumb to communism, had its roots in this period and ultimately led to the social, political, and military quagmire of Vietnam.⁷

Orwell's 1984, published in 1949 as the Cold War unfolded, struck a nerve as readers measured their current insecurities against a date that seemed so far away. Orwell's villain was the faceless bureaucrat in the totalitarian state, where government kept every aspect of citizens' lives under constant surveillance. The villain's accomplice was technology, personified by "Big Brother":

The poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. "Big Brother Is Watching You," the caption beneath it ran . . . [In the apartment] the telescreen received and transmitted simultaneously. Any sound . . . would be picked up by it. . . . There was of course no way of

knowing whether you were being watched at any given moment.⁸

Technology had helped the United States end World War II: The atomic bombs dropped on Japan were an awesome expression of it. Rocket technology acquired from the Germans by the United States and the Soviet Union fueled a Cold War duel in which the two postwar superpowers raced each other to outer space. The race for space became a scorecard, stunning Americans when a Soviet rocket hurled a basketball-sized sphere dubbed "Sputnik" into Earth orbit.

The competition had its down side, despite the technological advances and prosperity spawned by it. In addition to launching satellites and space capsules, the technology gave the superpowers the ability to hurl nuclear warheads across oceans, rendering border defenses and natural barriers obsolete. The threat of Soviet missiles added to the insecurity of Americans already unsettled by what they perceived as internal as well as external threats from communism. While technology, much of it developed during the war, had helped bring Americans postwar prosperity, it also held a sword over them.

World War II spurred other less spectacular but important technological innovations, such as the primitive computer, first used in 1944 to calculate weapon trajectories for the Navy.⁹ In 1947, the transistor was invented. The device--a tiny piece of silicone that could mimic the vacuum tube--replaced its bulky glass counterpart

used in early computers and formed the embryo for the development of the modern digital computer.¹⁰ Vacuum tubes, and later transistors, functioned as electronic on-off switches that allowed scientists to string together numerous simple tasks--the basic function of computers. Eleven years after the transistor was invented, the modern computer was born with the development of the integrated circuit. This pivotal innovation allowed thousands of transistors and other components to be strung together on a single piece of silicone. The results were computers that could complete vast numbers of simple tasks in a short time.¹¹ As the 1950s waned, the information gathering and processing potential of the infant computer technology began to be realized by scientific and social planners in business and government.

The development of computer technology coincided with another development, which had its roots in the Great Depression--the rise of the social welfare state. The New Deal, which Franklin Roosevelt christened in 1933, was based on the assumption that lawmakers should provide social and economic security to those displaced by an impersonal industrial system and that administrative agencies should facilitate this process. The expansion of administrative authority extended the reach of federal laws into the lives of millions of citizens who came to the government seeking help and benefits as well as those subject to a growing number of federal regulations.¹² It also reflected a basic

change in the way legislatures and courts distributed economic risks and benefits throughout society. Government no longer simply enhanced economic opportunity by standing aside; instead, it assumed the affirmative role of ensuring certain rights and liberties.¹³

As the 1960s matured, government in the role of benefit provider grew rapidly under President Lyndon Johnson's Great Society Program.¹⁴ With this expanding role, government developed parallel needs for vast amounts of personal information from those who sought benefits. In exchange for benefits, citizens were asked to relinquish personal data to support their claims.

Also during the 1960s, business and social planners grew increasingly enamored with the science of systems analysis. This computer-assisted process involved the mathematical simulations of complex activities. Systems analysis allowed planners to study vast amounts of related information and from it reach sophisticated conclusions for dealing with government programs and setting policies. In addition to management of the Vietnam war effort, which Secretary of Defense Robert McNamara attempted to control with the lock-step precision of a Ford Motors assembly line,¹⁵ systems analysis was applied to an array of social problems, including health care delivery, urban transportation, and higher education. The management tool gave business and social planners sophisticated and

economical means of gathering and sorting data and evaluating programs and institutions. In the social welfare sphere, systems analysis required the gathering and storage of data on millions of people.¹⁶

Demand generated by the uses of personal data, and the systems necessary to store and process that data, posed a challenge to the conventional social and legal means of protecting individual privacy. Current laws and regulations, written when paper record systems were cumbersome and decentralized and, thus, naturally ensuring at least some degree of privacy, appeared inadequate to deal with the new issues and threats to personal liberties.¹⁷

Obviously, several forces were at odds in the 1960s as the computer privacy issue was thrust into the public arena. Concern about totalitarian government was a major theme, reflected in the actions of government, the courts, and the press. Orwell's 1984 showed how technology could be mastered by an unscrupulous government to undermine the individual. And the rampant growth of the federal bureaucracy and its appetite for information gave the newly developing computer technology a starring role. But the theme that seemed to most capture the popular imagination was the computer cast in the role of "Big Brother."

The Computer Issue Unfolds in the Media

Concerns about the threat of government computers to personal privacy punctuated much of the popular and

scholarly literature about the new technology throughout the 1960s and early 1970s. Earlier books, such as 1984 and Aldous Huxley's Brave New World,¹⁸ once treated as science fiction, achieved new relevance. Several books in the early 1960s, such as Vance Packard's The Naked Society, addressed in general terms technological advances and the dangers and pressures they imposed on society.¹⁹ One author, viewing computers from a practical rather than futuristic perspective, suggested they had human-like qualities:

They are beginning to operate the way man appears to when he is exploring ways of solving a novel problem. That is, they apply and modify, as appropriate, previous experiences with the methods of solution for what appear to be related problems. Some of the machines show originality and unpredictability.²⁰

The popular film "2001: A Space Odyssey," with its anthropomorphic computer "HAL" defying his designers and commandeering the space station he was programmed to protect, brought the notion of a thinking computer into the popular culture.²¹ One commentator on the social effects of computer technology took issue with the cinematic portrayal of a "thinking" computer: "All too often we fall prey to the fallacy that computers live in their own self-contained world, functioning independently and beyond the control of man." Referring to HAL, the "neurotic but domineering computer in 2001," he cautioned that computers are no better or worse than the humans who program them.²²

Many books that addressed computer concerns during the 1960s and 1970s, however, focused on fears related to computer privacy and other dangers technology posed for civil liberties. The focus of much concern was a proposal by the federal Bureau of the Budget for creation of a National Data Center. Such a center would bring together information gathered by various federal agencies--much of it personal in nature--in a centralized computer system. The National Data Center proposal died after House and Senate hearings in the mid-1960s. The proposal will be detailed in the next section, which looks specifically at those hearings.

Among the most influential writers was law professor Arthur Miller, whose book The Assault on Privacy²³ helped define the computer privacy debate and whose later testimony was the centerpiece of several congressional hearings. In his book, Miller suggested that

Already there is a growing awareness of the effects that certain applications of the computer may have on that elusive value we call "personal privacy." In the past the very ponderousness of movable-type technology inhibited man's urge to collect and preserve information about his peers and thereby served to limit the amount of data that was recorded about individuals. But many people have voiced concerns that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of casual observers, including the morbidly curious and the maliciously or commercially intrusive.²⁴

Alan Westin was another influential writer during the period. His book Privacy and Freedom cautioned that a centralized computer, with access to various files on individuals, could combine and analyze files with an efficiency that would decimate traditional expectations of privacy.²⁵ To put the computer privacy threat into perspective, Westin calculated that, in 1972, computer technology existed that could maintain on-line files containing the equivalent of 20 single-spaced typed pages of personal information on every man, woman, and child in the nation.²⁶ He also noted, prophetically, that even absent a National Data Center, separate computer systems could be interconnected to create a de facto national data bank.²⁷

David Linowes, who would later chair the 1977 U.S. Privacy Protection Commission, argued in "Must Privacy Die in the Computer Age?" that the substantial social and economic benefits realized from increasingly sophisticated computer technology had been achieved with a substantial loss of personal privacy.²⁸ Jerry M. Rosenberg, the author of The Death of Privacy, suggested that if there were no safeguards on the collection and use of computerized personal information, "the right 'to be let alone' may be slipping away without public protest."

Issues raised by the National Data Center proposal were addressed in several scholarly articles. Arthur Miller's "Personal Privacy in the Computer Age: The Challenge of New

Technology" suggested that computers helped to improve society but that safeguards against abuse and misuse of personal information posed serious problems.³⁰ Richard Ruggles, in "On the Needs and Values of Data Banks," explored the practical and ethical dimensions of the accumulation of personal information in government computers.³¹ David L. Bazelon, in "Probing Privacy," noted that privacy, with respect to computerized government information, was best conceptualized in terms of an ongoing tension between individual privacy and the public's right to know about the activities of government.³²

Constitutional scholar Harry Kalven, Jr., whose work influenced generations of legal thinkers, looked ahead more than a quarter of a century in a 1967 article titled "The Problems of Privacy in the Year 2000." He foresaw how advances in technology could threaten personal privacy--especially the growing efficiency of government computers. Said Kalven,

When, as is likely, this technological efficiency is coupled with the government's ever increasing demands for special information, the prospect is one of a formidable dossier on every member of the society. Information may initially be collected for relatively innocuous purposes such as income tax, social security, special aid programs, and special support for education. . . . At some happy future moment, all of this information could be combined with the FBI files so as to produce a devastatingly detailed and accurate profile of each member of society. The disturbing result could be that everyone will live burdened by an unerasable record of his past and his limitations. In a way, the threat is that

because of its record-keeping the society will have lost its benign capacity to forget.³³

Articles in the popular press during the 1960s show that the nature and tone of public discussion about computers in society shifted dramatically over a relatively short time. At first, the popular press, as well as various technology-related trade publications and journals, heralded advances in computers and reflected a general infatuation with the new technology and its seemingly boundless promise as a tool of science, government, and business. An example of the early approach to computers in the popular literature appeared in Time in April 1965. The weekly news magazine devoted its cover story to "The Cybernation Generation," which touted the benefits of computers to society. The article quoted a General Electric vice president who proclaimed that "the electronic computer may have a more beneficial potential for the human race than any other invention in history."³⁴

But then the nature of articles about computers began to change. Instead of touting the computer's potential, articles focused on the potential social consequences of an unbridled technology in the hands of the unwitting or unscrupulous. The change coincided with a growing concern about the proposal for creation of a National Data Center to pool information from various government agencies.

As the debate over the proposed National Data Center quickened, the Orwellian specter of "Big Brother" grew. A

year after the Time article heralded "The Cybernation Generation," U.S. News & World Report cautioned in a centerpiece story that "your life story may be on file with the Government before long, subject to official scrutiny at the push of a button."³⁵ In the article, Dr. Orville G. Brim, Jr., chairman of the Russell Sage Foundation of New York, likened the proposed National Data Center to a "government dossier bank." He said there was no doubt society could be run better with the personal information a data center would gather and store. But he cautioned that "we must protect the individual against the chance of raiding parties by unscrupulous politicians."³⁶

Newsweek, responding to hearings before a U.S. House of Representatives subcommittee on the National Data Center proposal a few months later, echoed the arguments against the center. Citing 1984, the article noted that the ominous date was only 18 years away.

Or maybe less. At least twenty Federal departments and agencies regularly collect and store pertinent information--much of it unevaluated--on U.S. citizens. And last week, the Budget Bureau was pushing a scheme to gather all data collected by Federal bodies into one centralized computer system.³⁷

Social critic Vance Packard, who testified at the National Data Center hearing, worried that technology in the wrong hands could seriously undermine fundamental social values. Evoking an image of an individual entangled in reels of computer tapes, he cautioned that "some relentless

bureaucrat . . . could lead us to that ultimate of horrors, a humanity in chains of plastic."³⁸ Packard also noted that computers could erase any opportunity an individual might have for a second chance in society, a theme that other critics of computerized data banks sounded and that the Supreme Court adopted almost a quarter of a century later. Computers, Packard said, were incapable of making allowances for earlier human mistakes and that the "Christian notion of the possibility of redemption is incomprehensible to the computer."³⁹ Arthur Miller observed in The Atlantic that computer technology already had reached the point that vast amounts of personal information could be controlled by government. "The computer science is already so advanced that experts envisage a huge National Data Center to speed and simplify the collection of pertinent information about Americans," he said.⁴⁰

Perhaps most indicative of the growing public awareness of computer privacy concerns was a special issue of Saturday Review devoted to the "potentiality of the automation revolution and its implications for our society." The series of eight articles, plus an editorial titled "The Computer and the Poet," began with the conclusion that

Few technological developments are formidable enough to mark turning points in human history. Two such phenomena have occurred in our time: the atomic bomb and the computer. [If] the implications of the bomb are beginning to be understood . . . the implications of the computer as yet are only faintly comprehended.⁴¹

Even if this warning salvo by the highbrow Saturday Review were fired over the heads of most average Americans, it scored an immediate and direct hit on one group of public policy makers. The articles would become Appendix 3 of The Computer and Invasion of Privacy hearings before a Subcommittee of the Committee on Government Operations of the House of Representatives.⁴² The subcommittee began hearings on the computer-privacy issue two days after the articles were published. The hearings, spawned by concerns about the effect of technology on society, set the tone for a public policy debate that ultimately led to congressional action to harness the threat of computer technology.

Hearings on Creation of a National Data Center

In 1965, the U.S. Bureau of the Budget floated the proposal for creation of a National Data Center. As envisioned, the center would pool data from a score of federal agencies in a centralized computer system. The goal of such a center was to improve government efficiency by bringing together and standardizing the increasingly decentralized record systems of various federal agencies at a time when demands for information in social planning and benefit allocation were rapidly growing.

The genesis of the National Data Center concept was at the 1959 convention of the American Economic Association (AEA), which addressed the need to preserve data for economic research. The government collected economic and

related data as part of its regulatory function, and AEA was concerned that without a program to maintain such data it would be lost for future research.⁴³ To this end, the AEA recommended that the nonprofit Social Science Research Council, which represented the interests of social scientists, conduct a feasibility study. The study was begun in December 1960.

Chaired by Richard Ruggles of Yale University's Department of Economics, the Social Science Research Council made an agency-by-agency study of the federal government during the next three years. Ensuring access to data for scientific purposes became a primary concern of the council, which approached the Bureau of the Budget and the National Archives for assistance with the study. The Bureau of the Budget and the National Archives surveyed about 20 government agencies on the amount of machine-readable data they held and found that the agencies stored and analyzed data in many different ways. The Ruggles committee discussed problems inherent in government and nongovernment disclosure, since much of the information was confidential in nature. But the committee concluded that identifiable personal information could be sufficiently masked to protect privacy. The Ruggles committee concluded that

because of the decentralized nature of the federal statistical system and the pressure of the primary functions of the agencies, neither outside scholars nor Federal agencies are able to utilize efficiently the large amount of information which has been obtained at public expense. Therefore,

the committee urged that a federal data center be established by the federal government. Its purpose would be to preserve and make available to both government and non-government users basic statistical data that originated at all federal agencies.⁴⁴

The Ruggles committee turned over its report to the Social Science Research Council in early 1965. Based on its conclusions, the Bureau of the Budget, which had joined the project at the research council's request, hired a private consultant to review the concept of a National Data Center. Edgar Dunn, Jr., of the consulting firm Resources for the Future, Inc., issued his report in November 1965. Dunn concluded that computers could be used effectively for public policy analysis and that "the concept of a National Data Center is an appropriate vehicle for program reform."⁴⁵ As envisioned by Dunn, a National Data Center would be responsible for the following:

1. File storage and management of significant archival records.
2. A central referral and reference source for the users of federal statistics.
3. Explicit facilitating services for the users of federal data such as file rearrangement, tape translation, record matching, disclosure by-passing, and performance of standard statistical routines.
4. Development of computer hardware and software systems.
5. Provision of staff support to work in conjunction with the Bureau of the Budget to develop and establish standards essential to system capability.⁴⁶

Responding to concerns that a National Data Center could be used to monitor the personal lives of individuals, Dunn said that danger could be averted in two ways. First,

Congress could legislate statutory restrictions on use of the information. Second, he said, computer systems could be designed to require code books to ensure that only designated persons would have access to the system.⁴⁷

A special committee was established by the White House to review the proposal. It was headed by Carl Kaysen, a former Kennedy administration economist and chairman of Princeton University's Institute for Advanced Study. Kaysen's report endorsed the National Data Center proposal and suggested that it also include state and local government data.⁴⁸

For the National Data Center to work, the Bureau of the Budget conceded, people on whom data were collected must be individually identified in some way; precautions would be taken, however, to prevent the disclosure of any confidential information.⁴⁹

Congress responded quickly to the National Data Center concept. In 1966, the House Committee on Government Operations' Special Subcommittee on Invasion of Privacy held hearings on the data center proposal.⁵⁰ They were a continuation of a special inquiry initiated the year before by Rep. William L. Dawson, chairman of the House Committee on Government Operations. Dawson's committee dealt with several broader issues related to technology and personal privacy.⁵¹

During the National Data Center hearings, the conflict between two important public policy considerations became apparent. Proponents of the data center echoed conclusions of the earlier Ruggles committee and Bureau of the Budget consultant's reports. They emphasized that the current decentralized system was cumbersome and inefficient and impaired federal agencies' ability to plan effectively and provide services efficiently. In sum, they argued that government could be run better with such a data system. Opponents of the data center proposal countered with the possibility that personal information in a centralized computer might be abused or misused in ways that violated personal privacy. To them, the proposal left too many questions unanswered.

Subcommittee Chairman Cornelius Gallagher of New Jersey opened the hearings by acknowledging that technology over the centuries had enriched societies. A National Data Center, he said, would undoubtedly "add to this enrichment" by streamlining government. But he also envisioned a potential problem:

Just as democratic governments historically have secured the freedom of their citizens partly by controlling the fruits of scientific progress, so too must we now make sure that government computers do not provide the means by which federal officials can intrude improperly into our lives.⁵²

Gallagher said the goal of the hearings was to create "a climate of concern" to ensure the privacy of individuals

while weighing computer privacy concerns against the need to foster government efficiency.⁵³ He called for a "sense of balance," noting that a data bank's benefits to researchers, for example, could be realized while "human dignity and civil liberties" were preserved.⁵⁴ Yet, he remained wary of such a powerful tool and of the power it would render to those who mastered it:

The possible future storage and regrouping of such personal information also strikes at the core of our Judeo-Christian concept of "forgive and forget," because the computer neither forgives nor forgets. We are told that the computer can be programmed to program out derogatory and confidential information; what we fear is the ability to program it in.⁵⁵

In opening this discussion, Gallagher also wondered whether, indeed, the two conflicting interests--government efficiency and personal privacy--could be reconciled. He said the issue was not whether a National Data Center would be beneficial; obviously, it would. Said Gallagher,

A statistical data bank can be established and great benefits derived from it. However, there appears to be a great imbalance between technology on the one hand, and the law and public interest on the other. The issue is, therefore, can we achieve a balance so as to assure that technological progress will serve man and that man's free will will dominate the new environment that the computer is rapidly bringing about?⁵⁶

Subcommittee member Benjamin Rosenthal of New York posed the computer privacy question in terms of a balance between two important social considerations: "Does the additional knowledge we might gain yield benefits to society greater than the losses to the individual?"⁵⁷

In testimony before the committee, several themes and arguments emerged. Subcommittee member Frank Horton of New York said arguments that the information already existed in other forms and was accessible were specious and obscured the dangers inherent in a centralized data center, where time and distance no longer afforded people a measure of anonymity. In comments that the U.S. Supreme Court would later echo in a case addressing the proper legal limits on computerized personal information, Horton observed, "Information is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard."⁵⁸

The leadoff witness before the committee was novelist and social commentator Vance Packard, whose writings had questioned the effects of technology on fundamental social values. He warned the committee of the danger of "depersonalization" resulting from the use of computers and of humans being "processed" like a commodity and treated as objects instead of living, breathing beings.⁵⁹ Such a center, Packard predicted, would foster a totalitarian atmosphere creating the stifling impression that "somewhere there is an all-seeing eye."⁶⁰ Several other speakers voiced similar concerns.

Packard also pointed out that the threat to individuals need not come from overzealous or corrupt public servants;

inadvertent data-processing mistakes, perpetuated in government data banks, could ruin careers and lives. This potential was greatest, he said, when all kinds of raw information was fed into computers, without explanations, corrections, updates, or reference to extenuating circumstances.⁶¹

Similarly, Charles A. Reich of the Yale Law School questioned the initial quality of the information gathered about individuals. He worried that the methods of gathering information, before it becomes part of a computer data base, may themselves be suspect: "I am talking about the kind of things that ask for more than we know and then make it into the truth."⁶² He noted that as information gets farther in distance and time from its original source, it becomes less and less accurate "until what was the truth can become a lie."⁶³ Reich also raised a fundamental constitutional issue--the right under the Sixth Amendment of individuals to confront their accusers. He said that maintaining a National Data Center, in which case individuals might not know what is in their computer files or what judgments are being made about them on the basis of those files, would constitute a "denial of the constitutional right to confront . . . those who make statements about you, to question them, to rebut, to answer. . . ."⁶⁴

The first witness to testify in support of the National Data Center proposal was Raymond T. Bowman, assistant

director for statistical standards for the Bureau of the Budget. Bowman, in charge of making recommendations on whether the center should be established, said electronic data processing had revolutionized government record-keeping. The Bureau of the Budget, he said, was committed to making sure that technological advances in data processing resulted in more effective use of statistics to deal with problems confronting the nation and in reducing the burden on people giving information to government. "More and more we are coming to realize that the problems with which we must deal are combinations of many factors and can only be diagnosed and solved by information which relates the various factors involved," he said.⁶⁵

Bowman conceded that much of the information government needed to function effectively was personal, that individuals had to in some way be identified to make the coordinated analysis of the information useful. But he discounted the notion that such identification would necessarily violate privacy. He said, "The development of a statistical data center need not pose a threat to individual privacy if such a center is governed by restrictions that prevent the release, either to persons within Government or to persons outside Government."⁶⁶ Bowman pointed out that under federal laws and agency regulations, information reported to the government by individuals or businesses for statistical purposes could not be released in ways that

identified the provider. "There is general recognition that this practice of confidentiality is sound public policy. . . . Maintenance of this principle would be a major tenet of any statistical data center and is clearly required by law." ⁶⁷

Edgar S. Dunn, Jr., the research analyst for the firm that prepared the report for the Bureau of the Budget, confronted the public's fears of "Big Brother" head on.

The lay or public image of such a system is one of an automated monster with everybody's record that can be instantaneously retrieved by pressing buttons. There seems to be no awareness that the same technology that projects this frightening image has characteristics that can be utilized effectively to protect the sanctity of the individual record.⁶⁸

Dunn said much of the public's misconception was based on a misunderstanding of government record systems. He noted there were basically two different types of record systems. The first was a statistical information system, similar to that envisioned in the National Data Center proposal. Under it, statistics would be gathered that did not relate to any particular individual. It would identify only characteristics that related to groups or populations. The second kind of system was an intelligence system for gathering information about specific individuals. He noted such systems were common and essential in private and public business but were not related to what the National Data Center had in mind.⁶⁹ Dunn said privacy protection within any government record system had two components--statutory

safeguards and those stemming from the design and technical characteristics of the systems. He noted that the very technology distrusted by many critics of a data center could be used to shield personal information from those who lacked the statutory authority to see it.⁷⁰

One of the strongest proponents of the National Data Center was John W. Macy, Jr., chairman of the U.S. Civil Service Commission. Although Macy did not appear before the committee, his magazine article in Saturday Review on the great value of "automated government" became part of the hearing record. In the article, Macy emphasized the positive qualities computers offered a society: "This seems to me to be the answer to those who fear that computers will de-emphasize humanity. Far from it! By removing the clerical decisions and the mass of paperwork details the computer may well free the mind of man for more worthy use."⁷¹ Macy maintained that centralizing data would, simply, broaden the horizons of knowledge, create greater efficiency and save substantial amounts of time and money.⁷²

The Senate also addressed the National Data Center proposal. However, its hearings before the Judiciary Committee's Subcommittee on Administrative Practices and Procedures were brief compared to those in the House.⁷³ The hearings consisted primarily of testimony from Edgar Dunn, Jr., and, as in the House, subcommittee members expressed worries that technology might run roughshod over individual

liberties. They made it clear that proponents of a data center bore the burden of allaying such fears.

Subcommittee Chairman Edward Long of Missouri opened the hearings by acknowledging the difficulty of the task. The proposal for a "single machine-age information reservoir" to replace "bits of information on an individual being stored in a number of files and archives throughout government" raised hard questions, he said.⁷⁴ What would be its effect on American citizens? Could a system not meant to deal with specific individuals, but which out of necessity must identify them, be used to create dossiers? Where would the information gathering stop? These questions must be answered, Long said.⁷⁵

Dunn again attempted to counter the perception that the proposed data center would threaten privacy, emphasizing it would not be interested in potentially damaging information, such as court records, but in general purpose statistics. He said that the proposal was consistent with ongoing agency record practices. And he argued that government had an urgent need for the compiled information for intelligent public planning, administration, and program evaluation.⁷⁶

Chairman Long concluded that the discussion of the data center proposal was only a starting point. "It could become a Frankenstein of such proportions that we think it requires a great deal of further study," he said. "There are problems this committee feels should be raised in the

Congress, and the administration should take a careful look at it."⁷⁷

Committees from both House and Senate held a second round of talks the following year, revisiting some of the central issues.⁷⁸ But the proposal died. Uncertainty about new computer technology won the day and would continue to underscore congressional thinking for decades to come.

Yet, technological advances eventually created a de facto data center within the federal bureaucracy. And Congress responded with passage of the Computer Matching and Privacy Act, discussed later in this chapter.

The Computer and the Bill of Rights Hearings

In 1971, uncertainty about the effects of computers on personal privacy remained alive and well--this time before the Senate Judiciary Committee's Subcommittee on Constitutional Rights.⁷⁹ The hearings on Federal Data Banks, Computers, and the Bill of Rights set out, in the words of Chairman Sam Ervin of North Carolina, "to apply the harness and rein to computer and information technology."⁸⁰ Noting that in the computer age budget requests for computer systems were not "necessarily akin to requests for rubber bands," Ervin maintained that the time "to ask questions and obtain answers is before the automated systems are installed and before the experts and specialists take over."⁸¹ He surmised, "If Americans can harness computers to

get to the moon, surely we can harness them to preserve our liberty."⁸²

The hearings addressed a broad range of activities and rehashed many of the arguments for and against computerized government information raised during the National Data Center hearings, and they laid the foundation for the Privacy Act of 1974.

In his initial remarks, Senator Ervin spelled out the motivation for the hearings and what he hoped to achieve.

These hearings were called because it is clear from the complaints being received by Congress that Americans in every walk of life are concerned about the growth of government and private records on individuals. They are concerned about the growing collection of information on them which is in the hands of those whose decisions can affect their lives for better or worse.

They are concerned that they are constantly being intimidated, coerced, or pressured into revealing information to the wrong people, for the wrong purposes, at the wrong time.

They are concerned that this information is being automated or computerized without proper screening or controls.

But, above all, they are worried that the existing laws are no longer sufficient to protect the privacy of the individual against the "information power" of government.⁸³

Ervin acknowledged the important benefits of the new computer technology in an increasingly complex society where government needed vast amounts of personal information to help it govern wisely and efficiently.

Throughout our Nation, the managers of government and private organizations, political officeholders, and members of legislatures have besought the aid of science and technology to increase their capacity to gather, store, and use

information about people. To help in the business of governing and managing, they have pressed into service the wonders of our scientific age.⁸⁴

But Ervin emphasized that "the blessings of this computer age are not unmixd," noting that concerns had been expressed to Congress by the person who

must now fear not only the human quirks and errors involved in paper dossiers, but also the mechanical quirks and errors. He must worry about denial of substantial benefits and privileges because of computer breakdowns, or the stealing of personal records because of the access and taping afforded by improperly guarded computer systems. He must deal with automatic responses of computerized record systems for purposes such as credit checking.⁸⁵

Ervin pointed out that the source of public anxiety over computers was not distrust of government per se; instead, concerns about informational privacy stemmed from the rapidly growing complexity of society, which "constantly produces new problems which must be solved by Congress and State legislatures. These bodies have more need than ever before for accurate information on which to legislate, and to legislate wisely."⁸⁶

To sum up the dilemma, Ervin quoted the work of Alan Westin, editor of the New York City Bar Association's report Privacy and Freedom, who lamented the by-gone days when business was conducted in person:

The more computers offer opportunities to simulate behavior, forecast trends, and predict outcomes, the more pressure is generated for personal and organizational information to be collected and processed. In a way we sometimes only dimly grasp, this is one of the great changes in modern society. At the same time, and partly

generated by this change itself, there has been a distinct rise in public fear of depersonalization and manipulation through collection and processing of information. Big government, big private employers, even big social science, have replaced the softening, face-to-face aspects of social control of earlier times. In this setting, the private personality is the last defense of individuality, the ultimate shield of personal autonomy. To the extent that this public fear clashes with the new information theory adopted by the decision-making elites of the society, this produces a sharp conflict that puts special stress on a society that wants to support both science and liberty.⁸⁷

The first witness at the hearings was Arthur Miller, author of The Assault on Privacy who had been a key witness before the 1966 House hearings. He began his testimony by observing that "Americans today are scrutinized, measured, watched, counted, and interrogated by more governmental agencies, law enforcement officials, social scientists, and poll takers than at any other time in our history."⁸⁸ In addition, he emphasized that more information was gathered in the United States than in any other nation and that information gathering and surveillance were being expanded to such a degree that basic rights, such as privacy, were at risk.⁸⁹

Miller noted that science fiction had begun to ring true. "Unfortunately, few people seem to appreciate the fact that modern technology is capable of monitoring, centralizing, and evaluating these electronic entries, no matter how numerous they may be, making credible the fear

that many Americans have of a womb-to-tomb dossier on each of us," he said.⁹⁰

Miller surmised that the general lack of concern about government information-gathering reflected the fact that, for the most part, such activities were well-intentioned. But, invoking the concerns of Orwell and Huxley, Miller nonetheless expressed fear about the cumulative negative impact on the public's "state of mind," similar to that caused by the invidious technology in 1984.

In the past, dictatorships always have come with hobnailed boots and tanks and machine-guns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressing, just as chilling and just as debilitating on our constitutional protections.⁹¹

Miller, discounting assertions by witnesses at earlier computer-privacy hearings that laws were adequate to ensure privacy, concluded that the existing legal framework failed to deal with privacy issues raised by computers and data banks. He said the common law of privacy had as its model the mass dissemination of personal facts in a news medium, not a computer.

The entire concept of personal privacy as developed by the courts has been in reaction to the media of mass communication. It may be adequate when you are talking about information that is disseminated openly in the public press, because the individual has a chance of seeing, responding to, and if he feels aggrieved, of taking the publisher to court. But I think one of the differences . . . of the modern information pattern is that you are not dealing with mass dissemination. . . . You are dealing with records that are kept and stored in electronic form in the bowels of some Federal agency or some State agency

or some corporation or some university, of which the citizen simply has no knowledge. . . . In other words, the person most concerned about the information . . . has least access to it.⁹²

Miller said the federal government had numerous scattered statutes for protecting private personal information but that many of them were little known. It was asking too much, he said, to depend solely on the bureaucrats to know the various laws and regulations and to honor them. He added that common law privacy rights and existing statutory protection from the Freedom of Information Act, the Federal Reports Act, and the General Services Administration regulations were not "sufficient to strike a balance between the individual and the society in terms of information."⁹³ To strike this balance, Miller suggested, Congress should study the problem and enact legislation responsive both to the concerns of agencies, with their vital needs for meaningful information, and to individuals about whom information was gathered and maintained.⁹⁴

Dr. Jerry Rosenberg, a psychologist, echoed some of Arthur Miller's concerns about the cumulative effect of technology on the public psyche. Rosenberg warned the committee about the psychological impact of rapid technological change. He said his studies had found Americans concerned about the "undemocratic process which starts at birth to make people believe that they are unable to say 'No' to divulging personal information." This

inability to say 'No' perpetuates the collection of data "that will follow them for the remainder of their lives--frozen in time and in the computer."⁹⁵ Rosenberg offered the example of a teenager who had a minor scrape with the law. "Today, this kind of behavior is not easily forgotten. Our minds forget, computers do not. . . . It is still part of the permanent record of your behavior."⁹⁶

While the Ervin subcommittee hearings had no immediate result, they did lay the groundwork for legislation the chairman soon proposed to place limitations on the use of personal information by government.⁹⁷ The hearings, along with those preceding them, also apparently attracted the attention of some members of the federal bureaucracy. At least one agency, the Department of Health, Education and Welfare, acted independently to ensure that personal information was not abused.

The Health, Education, and Welfare Report

Against a backdrop of growing concern about the privacy implications of computerized government records, the secretary of the Department of Health, Education and Welfare (HEW) initiated a study of agency practices. Caspar Weinberger established an Advisory Committee on Automated Personal Data Systems to explore the "relationship between individuals and record-keeping organizations" and to analyze several issues.⁹⁸ The committee, consisting of members from the social service professions, the research community,

academics, private industry, and government, was asked to make recommendations about

- Harmful consequences that may result from using automated personal data systems;
- Safeguards that might protect against potentially harmful consequences;
- Measures that might afford redress for any harmful consequences;
- Policy and practices relating to the issuance of Social Security numbers.⁹⁹

The committee issued its report in May 1973 titled "Records, Computers, and the Rights of Citizens."¹⁰⁰ In a forward to the report, Secretary Weinberger said that computer-based record systems could be a powerful management tool "invaluable to hard-pressed decision makers" and that one of the greatest challenges facing government was "to improve the capacity to administer tax dollars . . . [by] attempting to eliminate ineligibility, overpayment, and other errors from welfare caseloads."¹⁰¹ But Weinberger was quick to caution,

Nonetheless, it is important to be aware, as we embrace this new technology, that the computer, like the automobile, the skyscraper, and the jet airplane, may have some consequences for American society that we would prefer not to have thrust upon us without warning. Not the least of these is the danger that some record-keeping applications of computers will appear in retrospect to have been oversimplified solutions to complex problems.¹⁰²

The committee recommended the establishment of a "Code of Fair Information Practices" to regulate the collection and use of personal information by federal agencies. The

code, which became a model for the Privacy Act of 1974, had five major principles:

- There must be no personal data record-keeping systems whose very existence is secret.

- There must be a way for an individual to find out what information about him is in a record and how it is used.

- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

- There must be a way for an individual to correct or amend a record of identifiable information about him.

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.¹⁰³

The proposed code called for computer safeguards for both administrative and personal data statistical systems.¹⁰⁴ Violations of the safeguards would constitute "unfair information practices" and be subject to criminal penalties and civil remedies. The committee report also concluded that existing privacy laws did not meet the needs for safeguard systems. It recommended Congress enact legislation to ensure that personal data used for statistical and research purposes be shielded from disclosure in identifiable form.¹⁰⁵ The committee also acknowledged public concern that Social Security numbers would be used to assemble dossiers on individuals from widely dispersed systems. It concluded that Social Security numbers were already being used as a de facto universal identifier and recommended steps to curb such practices.¹⁰⁶

Until legislative enactment of the recommended Code of Fair Information Practices, the committee said agency departments in the interim should use their administrative and rule-making powers to safeguard all information within the federal system and in other systems within the reach of the federal government's authority. Additionally, the committee urged state and local governments to act to protect personal information.¹⁰⁷

The Privacy Act of 1974

Within a year of the 1973 HEW committee report, Senator Sam Ervin and three other senators proposed legislation to provide an "Information Bill of Rights" for citizens and a "Code of Fair Information Practices" to regulate federal executive agencies. In June 1974, in the wake of the Watergate scandal and its graphic examples of government abuses, the Committee on Government Operations' ad hoc Subcommittee on Privacy and Information Systems began joint hearings with the Judiciary Committee's Subcommittee on Constitutional Rights, which was considering related legislation.¹⁰⁸

Senator Ervin, chairman of both subcommittees, announced the joint hearings in a speech before the Senate on June 11, 1974. He noted that his subcommittees had heard complaints about government information practices from witnesses from various walks of life and spanning several administrations. He said the complaints showed Americans

were more concerned than ever about the potential for government to abuse its power to investigate and store information. Said Ervin.

It is a rare person who has escaped the quest of modern government information. . . . When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.¹⁰⁹

Several witnesses spoke of the failure of legislation and judicial decisions to keep pace with the growing efficiency of computers and of the lack of clear safeguards. Alan Westin, director of the 1972 National Academy of Science project on computers and privacy, said it was essential to act immediately to protect personal data. He said systems were being added and expanded and that it would be costly to alter file structures and computer software after systems were in place to accommodate new security provisions. Westin cautioned that "these systems may become so large, so expensive, and so vital to so many Americans that public opinion will be put to a terrible choice--serious interruption of services or installation of citizen-rights measures."¹¹⁰

Arthur Miller also addressed the hearings, again speaking about the threat of new technology to individual freedoms, including speech, privacy, association, assembly, and the right to petition government. He noted that

Probably in no Nation on earth is as much individualized information collected, recorded and disseminated as in the United States. . . . I think if one reads Orwell or Huxley carefully, one realizes that "1984" is a state of mind. . . . I think it is this fear that presents the greatest challenge to Congress right now.¹¹¹

In the aftermath of the Watergate excesses and amid the long-festerling fears of many academics, commentators and legislators that computers were eroding personal liberties, Congress enacted the Privacy Act of 1974. The legislative history of the act stated explicitly its concern about the dangers inherent in the federal government's use of computers.¹¹²

The Privacy Act was designed to protect individuals by providing them with more control over the gathering, dissemination, and accuracy of information the government maintained about them. It established safeguards against unwarranted intrusions into privacy that paralleled those in HEW's "Code of Fair Information Practices."

The Senate report on the legislation noted that the purpose of the Privacy Act was to

promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use and disclosure of personal information about individuals . . . [and] to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government.¹¹³

In addition to the general gathering and storing of personal information, the Privacy Act also addressed ongoing concerns about the indiscriminate use of Social Security numbers to keep tabs on individuals receiving benefits from the federal government. To curb this practice, the act prohibited requiring Social Security numbers as a condition for receiving benefits, unless specified by statute. The prohibition also extended to state and local governments.¹¹⁴

The act established penalties for violation of its provisions. Unlike the Freedom of Information Act, which is a disclosure statute that provides only for legal action to compel disclosure, the Privacy Act provided for criminal sanctions.¹¹⁵

One provision established a Privacy Protection Study Commission which was to report in three years on the effectiveness of the legislation in remedying privacy concerns. The commission was established as a compromise between House and Senate versions of the Privacy Act legislation as an alternative to a standing executive branch oversight agency.¹¹⁶

In 1977, as a debate unfolded over the growing practice of matching computer records among federal executive agencies, the study commission issued its report concluding the Privacy Act had "not resulted in the general benefits to the public that either its legislative history or the prevailing opinions as to its accomplishments would lead one

to expect."¹¹⁷ The commission said the act was being applied loosely and from the agencies' point of view and that changes were needed to strengthen its provisions. A key concern of the commission was the Privacy Act's "routine use" exemption. This exemption gave agencies relatively broad discretion in deciding what information could be shared with other agencies.¹¹⁸ Based on this discretion, the Carter administration attempted to launch "Project Match," a program to compare agency data bases to root out benefit abuse. The ensuing debate over Project Match, an executive-level attempt to establish a de facto equivalent of the ill-fated National Data Center, led to passage of the Computer Matching and Privacy Act. This legislation is discussed in the next section.

The Computer Matching and Privacy Act

During the hearings over the proposal for a National Data Center in the 1960s, the major concern was the possibility that government agencies with access to a centralized data center would share or compare information to monitor specific individuals, in violation of their rights of privacy. During those hearings, Paul Baran of the Rand Corporation suggested that the potential for a de facto data center already existed. Even without a centralized data center, he said, agencies still might compare computerized data in ways that endangered personal

privacy.¹¹⁹ Time and technological advances proved this concern well founded.

In 1977, the Department of Health and Human Services (successor to HEW) instituted Project Match.¹²⁰ The legal basis for the program, under which agencies used their computers to cross-reference data from other agencies, was the "routine use" exemption to the Privacy Act, which agencies began to interpret loosely to allow such data sharing.¹²¹

Project Match was aimed at using agency computers to compare welfare rolls with federal payroll records from the Defense Department and Civil Service Commission to ferret out people on welfare who had incomes in excess of welfare guidelines. The goal was to save tax dollars by reducing welfare fraud, waste, and abuse. The General Accounting Office and the Office of Technology Assessment defined the computer matching process as follows:

Typically, Federal agencies use computer matching to locate an individual, verify eligibility for benefits, or to develop investigatory leads. There are several different computer-assisted techniques for identifying similarities and differences between records. With "classic" computer matching, a computer compares the records of two separate data bases looking for individuals (or organizations) that appear in both files. Typically, the data bases contain information on beneficiaries under two different government programs.¹²²

While computer matching had at times been praised by Congress, by inspectors general, and by the President's Council on Integrity and Efficiency, such matching also was

criticized as ineffective and a violation of privacy.¹²³ One assessment of Project Match concluded the program cost more than it saved. It also found that computer matching errors often subjected innocent welfare recipients to undue government scrutiny and harassment.¹²⁴

In the early 1980s, Congress' Office of Technology Assessment (OTA) also expressed concern about the ease with which personal information could be disseminated with the aid of computers. The OTA cautioned that computer technology was out-pacing government's ability to ensure individual rights. In a 1981 report, the OTA said that information normally discarded when records were in paper format was being retained in federal agency computers. In addition, the report expressed concern that computers were making data generally easier to gather and store and that new technology allowed for "instantaneous nationwide distribution."¹²⁵

The computer-matching controversy did not escape the notice of Congress. Based on the cumulative criticisms and concerns about computer matching, Congress held hearings on the dangers posed by the computer sharing of agency information. The hearings revisited many of the issues from the National Data Center debate of the 1960s.

As early as 1982, the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs held hearings on computer matching.¹²⁶

At that hearing, Wilbur D. Campbell, director of Accounting and Financial Management Division, General Accounting Office, testified that computer matching provided a powerful tool for improving government efficiency. "[W]e believe that computer matching can be a very cost-effective tool for detecting error and fraud in Government entitlement programs and for identifying actions needed to strengthen program controls," he told the committee.¹²⁷

However, the committee also heard testimony that echoed concerns about due process and the integrity of data stored in government computers. As an example of the pitfalls of computer matching, the testimony focused on a Massachusetts program that violated the due process rights of welfare recipients whose records were matched with those of private banks. The aim of the program was to identify welfare recipients whose assets exceeded the amount allowed by law. Without attempting to verify the computer match or notify the individuals they were under scrutiny, the state automatically sent welfare termination notices to more than 1,600 people identified as having too many assets.¹²⁸ Fifteen percent of the people who appealed the automatic termination found their files simply contained Social Security number errors.¹²⁹ John Shattuck, National Legislative Director of the American Civil Liberties Union, testified that in some cases money in joint accounts, not held entirely by welfare recipients, was included in asset

determination. Other funds were held in trust or for such things as funeral expenses.¹³⁰

In 1986, the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs held hearings on a Senate bill that proposed to place limits on computer matching.¹³¹ Ronald Plesser, testifying for the American Bar Association, suggested matching was widespread because "the routine use provision [of the Privacy Act] is so big an exemption you could drive a truck through it."¹³² The exact extent of computer matching within the federal government was unknown when the committee began its hearings. In a 1986 report, the Office of Technology Assessment offered an estimate of the extent of computer matching and suggested the difficulty of coming to grips with the complex issue. "It is difficult to determine how much computer matching is being done by Federal agencies, for what purposes, and with what results. However, OTA estimates that, in five years from 1980 to 1984, the number of computer matches has tripled."¹³³

In 1987, the House Subcommittee on Government Information, Justice, and Agriculture held hearings on computer matching.¹³⁴ Eleanor Chelimsky, director of GAO's Program Evaluation and Methodology Division, expressed concern about the lack of procedures regulating computer matching decisions.

[I]n examining how decisions about computer matches have been made, we noted a generally

informal approach. The agencies presently have only general guidelines for documentation and for what should be considered and how it should be considered in the match decision process. We found no specific written criteria for determining whether or not a proposed match should be implemented, little documentation of what has been considered, and wide variation in the use of systematic planning procedures for developing and implementing matches. We found that the existence of improved technological capacity, legislative requirements, the extent and magnitude of the problems that were experienced (for example, overpayments being made because of unreported deaths), and concern about detecting and preventing waste, fraud and abuse were more prominent in the agency decisionmaking than the quantification of costs and benefits. Indeed, our work clearly shows that decisions to perform or continue a computer match are often made without systematic considerations of those costs and benefits.¹³⁵

In 1988, Congress passed the Computer Matching and Privacy Act. The legislation reflected privacy concerns caused by the sharing of personal information among government agencies and the agencies' lack of procedures governing computer matches. It amended the Privacy Act to "regulate the use of computer matching conducted by Federal agencies or using Federal records subject to the Privacy Act of 1974."¹³⁶

The computer-matching legislation dealt with problems associated with abuse of the Privacy Act's routine use exemption by requiring that agencies establish written agreements specifying the terms under which computer matches would be done. It also prescribed due process rights for individuals by preventing agencies from taking adverse action against them until information was independently

verified and the subjects of a computer match given 30 days advance notice. To provide oversight, the act required that agencies publish matching agreements with other agencies, report all matching programs to the Office of Management and Budget and to Congress, and establish internal boards to approve all matching activities.¹³⁷

Other Legislation Concerned About Computers and Privacy

Since the National Data Center debate unfolded, Congress has passed several measures, in addition to the Privacy Act and the Computer Matching and Privacy Act, dealing with the potential threat of computers to personal privacy. Some of the legislation was aimed at the information collection and dissemination practices of government agencies, other legislation at private businesses under federal jurisdiction that maintain records on individuals.

Fair Credit Reporting Act

In 1970, Congress passed the Fair Credit Reporting Act,¹³⁸ in part because of testimony related to the debate over the proposed National Data Center. The testimony indicated that an unregulated computer network already existed among various credit bureaus, which freely shared lawfully obtained, personal information. The act, limited to reports for credit, employment, insurance, and related benefits, sought to protect personal privacy and avoid inaccurate reports. To these ends, it gave the public

access to credit reports and the ability to challenge data in credit files. The act required agencies to follow reasonable procedures to make sure data were accurate, and that the data were used properly.¹³⁹ Penalties included costs, actual damages, and legal fees. But there have been loopholes in the law, and the continued abuse of consumer credit information--including mistakes perpetuated in records--and of other personal information gathered and disseminated by private data vendors has been decried recently in Congress and in the media. The controversy has served not only to increase efforts to further ease consumers' access to information held by credit bureaus but also to increase fears about computer-held information.¹⁴⁰

Fair Credit Billing Act

In 1976, Congress passed the Fair Credit Billing Act to bolster consumer protections already afforded under the Fair Credit Reporting Act. The act required that a creditor respond to a concern about an inaccuracy in a credit file within 30 days, during which time the credit agency could not issue an adverse credit report.¹⁴¹

Family Education Rights and Privacy Act

In 1978, Congress passed the Family Education Rights and Privacy Act, or so-called "Buckley Amendment," out of concern for the potential misuse of information about students. The act allowed for the withholding of federal

funds from educational institutions violating its disclosure-limiting provisions.¹⁴²

Right to Financial Privacy Act

In 1978, Congress passed the Right to Financial Privacy Act to limit access to personal records held by financial institutions.¹⁴³ Congress acted in apparent response to the U.S. Supreme Court's decision in United States v. Miller, in which the court held that individuals retained no expectations of privacy for information voluntarily submitted to banks. Such records, the court reasoned, were outside an individual's "zone of privacy" and, therefore, were not protected from general disclosure to the government under the Fourth Amendment.¹⁴⁴

Justice Brennan, in a dissenting opinion to the 5-4 decision, argued that bank customers should have a reasonable expectation that information turned over to banks will be used only for banking purposes. Brennan cautioned that such threats to personal privacy were exacerbated by new technology and that the courts must "keep pace" with the threat. Said Brennan,

[the] depositor reveals many aspects of his personal affairs, opinions, habits, associations. Indeed, the totality of bank records provides a virtual current biography. . . . Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of constitutional protection of individual privacy must keep pace

with the perils created by these new devices.
(emphasis added)¹⁴⁵

The Right to Financial Privacy Act provided due process standards and placed limitations on law enforcement agencies. To obtain banking records, investigators must have the written consent of the subject of the records or obtain a subpoena, a court order, or a search warrant. In each instance, the subject must be notified. In all but the case of a search warrant, access may be challenged, and the subject may sue the government and the financial institution for civil damages. Fines of up to \$100 per violation may be imposed, as well as actual damages. If violation is willful, punitive damages may be imposed.¹⁴⁶

The Computer Crime Act

In 1986, Congress passed the Computer Crime Act, which prohibits unauthorized access and disclosure of information held in government computers.¹⁴⁷ Under terms of the act--which places emphasis on the form of the government records, not their content--federal employees who release information covered by the act face criminal prosecution. Several legislators, including Senator Charles Mathias of Maryland, expressed concerns that the Computer Crime Act might foreclose access to information even when the Freedom of Information Act mandated disclosure.¹⁴⁸ Additionally, because of the criminal penalties allowed under the Computer Crime Act, concerns have been expressed that government record-keepers would be more likely to err on the side of

nondisclosure when normally accessible records are held in computers.¹⁴⁹

Electronic Communication Privacy Act of 1986

The Electronic Communications Privacy Act was passed to protect the content of private communications, regardless of how the information was transmitted. The act's stated purpose was to "update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technology."¹⁵⁰ It protects all electronic communications, including fiber-optic transmissions, cellular telephone calls, electronic mail systems, computer-to-computer data transmissions, and remote computer services.¹⁵¹

Computer Security Act of 1987

Congress passed the Computer Security Act of 1987 to ensure the security and privacy of "sensitive information" held in federal government computer systems.¹⁵² The Computer Security Act defines sensitive information as any unclassified information in federal record systems that, if lost, misused, or accessed or modified without authorization, could adversely affect federal programs or the privacy interests of individuals.¹⁵³ The legislation defined the term "federal computer system" to include all federal agencies, contractors working for federal agencies, and other organizations that process information using a computer system to accomplish government functions.¹⁵⁴

The legislation resulted from, among other things, concerns by private information vendors that federal executive agencies were threatening to reduce or foreclose access to unclassified, public-domain information simply because it was held in computers.¹⁵⁵ The focus of concern was a 1986 executive order from the National Security Agency, the so-called "Poindexter Directive," which established guidelines for withholding unclassified information agencies deemed "sensitive." The data vendors, many on-line services through which clients gain access to data bases using computers, feared the Poindexter guidelines might be invoked to render information in their systems "sensitive" and inaccessible. Among the users of such data services are corporations, the news media, state and local governments, and the legal and medical professions.¹⁵⁶

Jack Simpson, president of Mead Data Central, Inc., a major vendor with such services as the legal data base Westlaw, observed that no "magical transformation" occurred when unclassified information was put into a computer.¹⁵⁷

Because of concerns expressed by information vendors and others about the dangers to access posed by the National Security Agency's "sensitive" designation, the House report on the legislation made clear the act's relationship to the Freedom of Information Act.

In order to ensure that the Computer Security Act is designed to protect and not restrict access to government information, specific provisions were added . . . which make it explicitly clear

that the [act] has no bearing on the public availability or use of information. The designation of information as sensitive . . . is not a determination that the information is not subject to public disclosure nor does such a designation bear on the determination to disclose. Information that requires protection while . . . being stored in a computer may nevertheless be public information under the Freedom of Information Act.

. . . this limitation on construction of the Act applies regardless of the medium in which information is stored. Thus, where the government is without authority to restrict or regulate the content or use of information that appears in newspapers, the government remains without such authority with respect to the same information . . . [in] a computer data base, optical disk, or other computer system storage medium.¹⁵⁸

Video Privacy Protection Act

In 1988 Congress passed the Video Privacy Protection Act, loosely referred to as the "Bork Bill," after news accounts of U.S. Supreme Court nominee Robert Bork's video viewing habits. The stories were based on computer printouts of Bork's video rentals obtained by the news media. Under the bill, disclosure of such computerized lists of viewer habits were prohibited.¹⁵⁹

Scales Tipped Toward Caution

Concern about government use of computers to store and analyze personal information arguably was an outgrowth of the nation's insecurities created by the climate of the decade following World War II. The proposal for a National Data Center galvanized the computer/privacy debate during the 1960s, spurred by scholarly writings and the popular press. Congressional hearings on computers and privacy

focused the issues and lay the groundwork for the Privacy Act of 1974 and its progeny.

The role of computers in the federal bureaucracy increased steadily through the 1980s, continuing the public discourse over the clash between technology and privacy begun many years before.¹⁶⁰

Serious worries about computers are now embedded in the congressional consciousness and legislative memory and have been a significant factor in the formulation of public policy in the regulation of federal information activities.

At times, as the foregoing review of privacy-related legislation suggests, strong concerns and fears about computers have tipped the scales steeply toward caution when attempts were made to balance privacy with competing social interests. While these privacy concerns were laudable and mostly well founded, they, nonetheless, reflect a deep-seated distrust of technology in society generally, and within Congress specifically. This concern has the potential to skew public policy at the expense of competing societal interests.

One social value especially at risk is public access to government information. Statutes developed to ensure public access to government information, written when most records were paper and when the physical limitations of time and space ensured a degree of privacy, are no longer adequate to resolve novel access issues raised by computer technology.

Will statutes such as the Privacy Act and the Computer Crime Act, which impose criminal penalties for the release of information, reduce legitimate public access as record custodians feel compelled to err on the side of nondisclosure? The answer to such questions lies in revisiting the Freedom of Information Act to make it more functional in the computer age.

Notes

1. See generally General Services Administration, Federal Equipment Data Center, Automated Data Processing Equipment in the U.S. Government (April 1990); General Services Administration, Office of Federal Information Resources Management, Microcomputer Survey Report (September 1988); D. Brundy, "Computers and Smaller Local Governments," 12 Public Productivity Review 184 (1988); Draemer, King, Dunkle & Lane, "Trends in Municipal Information Systems," Baseline Data Report 2 (Spring 1986).

2. Justice Department v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 762-780 (1989).

3. George Orwell, 1984 3 (1949).

4. Barbara W. Tuchman, The March of Folly: From Troy to Vietnam 245 (1984). In a speech in March 1948 in Fulton, Mo., Churchill referred to the "iron curtain" extended across Europe and suggested that no one knew "the limits, if any, to [the] expansive and proselytising tendencies" of the Soviet Union.

5. For an overview of the McCarthy phenomenon, see Mark Landis, Joseph McCarthy: The Politics of Chaos (1987); Edwin R. Bayley, Joe McCarthy and the Press (1981). See also Alan F. Westin, Privacy and Freedom 286-287 (1967). Westin discusses concerns about authoritarianism and technology in scholarly literature, science fiction, on television, and in such diverse sources as the Wall Street Journal, Playboy magazine and Consumer Reports.

6. See e.g., Dennis v. United States, 341 U.S. 494 (1951). See also John A. Gorfinkel and Julian W. Mack II, "Dennis v. United States and the Clear and Present Danger Rule," 39 Calif. L. Rev. 475 (1951).

7. Tuchman, The March of Folly at 262.
8. Orwell, 1984 at 4.
9. John W. Macy, Jr., "The Cybernation Generation," Time, April 2, 1965, at 85-86.
10. T.R. Reid, "Computerthink," 5 APF Reporter 3-7 (Winter 1983). See also Jeremy Bernstein, The Analytical Engine: Computers, Past, Present, and Future (1964).
11. Id.
12. Kermit L. Hall, The Magic Mirror: Law in American History 267 (1989).
13. Id.
14. See generally Eli Ginsberg, The Great Society: Lessons for the Future (1974); Marvin E. Gettleman, The Great Society Reader: The Failure of American Liberalism (1967).
15. Tuchman, The March of Folly at 297.
16. John T. Soma and Richard A. Wehmhoefer, "A Legal and Technical Assessment of the Effects of Computers on Privacy," 60 Denver L.J. 451 (1983).
17. Arthur Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers 210 (1971). In addition: When the Freedom of Information Act was passed in 1966, the federal government operated about 3,000 mainframe computers. See David Morrissey, "The Age of Electronic Government," presented at the 1990 Conference on Advanced Investigative Methods for Journalists, at 2. Twenty years later, in 1986, the federal government operated 22,000 mainframe computers. By 1990, that number had more than doubled to 48,000. See General Services Administration, Federal Equipment Data Center, Automated Data Processing Equipment in the U.S. Government (April 1990). Government use of smaller microcomputers has also increased rapidly, from 490,000 to more than one million just two years later in 1988. See General Services Administration, Office of Federal Information Resources Management, Microcomputer Survey Report (September 1988).
18. Aldous Huxley, Brave New World (1958).
19. Vance Packard, The Naked Society (1964). See also Victor C. Ferkiss, Technological Man: The Myth and the Reality (1969).

20. Donald N. Michael, Cybernation: The Silent Conquest 6 (1962).

21. 2001: A Space Odyssey (Metro-Goldwyn-Mayer 1968).

22. Miller, The Assault on Privacy at 2-3. Concerns about the quality of data were expressed during hearings over a proposal for a National Data Center. Such concerns also are reflected in modern computer parlance with the term "GIGO"--garbage in, garbage out. This means that poor input or programming results in poor output.

23. See generally Miller, The Assault on Privacy, supra note 17.

24. Id. at 3.

25. See Westin, Privacy and Freedom, supra note 5. While Westin was concerned about personal privacy, he nonetheless recognized that privacy interests must at times be balanced with other societal interests, such as access to government information.

26. Cited in Michael D. Rostoker and Robert H. Rines, Computer Jurisprudence: Legal Responses to the Information Revolution 229 (1986) at 229. Alan Westin and M. Baker, Databanks in a Free Society: Computers, Record-Keeping and Privacy 337-406 (1976).

27. Westin and Baker, Databanks in a Free Society at 321-330.

28. See generally David Linowes, "Must Privacy Die in the Computer Age?" 65 A.B.A.J. 1180-1184 (August 1979).

29. Jerry M. Rosenberg, The Death of Privacy 5 (1969).

30. See generally Arthur Miller, "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society," 67 Mich. L. Rev. 1091 (1969).

31. Richard Ruggles, "On the Needs and Values of Data Banks," in "Symposium--Computers, Data Banks, and Individual Privacy," 53 Minn. L. Rev. 211, 216 (1968).

32. David L. Bazelon, "Probing Privacy," 12 Gonz. L. Rev. 587 (1977). Bazelon was the chief judge on the D.C. Circuit of the U.S. Court of Appeals.

33. Harry Kalven, Jr., "The Problems of Privacy in the Year 2000," 96 Daedalus 876-879 (Summer 1967), quoted in

William Cohen and John Kaplan, Constitutional Law: Civil Liberties and Individual Rights 528-530 (2d ed. 1982).

34. John W. Macy, Jr., "Cybernation Generation," Time, April 2, 1965, at 84. See also J. Pfeiffer, "How Computers Will Change Your Life," McCall's, May 1965, at 34; "The New Computerized Age," Saturday Review, July 23, 1966, at 15; "How Computers Liven Management's Ways," Business Week, June 25, 1966, at 112; and M. Greenburg, "Uses of Computers in Organizations," Scientific America, Summer 1966, at 192.

35. "A Government Watch on 200 Million Americans?" U.S. News & World Report, May 16, 1966, at 56.

36. Id.

37. "Bureaucracy: Chains of Plastic," Newsweek, August 8, 1966, at 27.

38. Id.

39. Id.

40. Arthur Miller, "The National Data Center and Personal Privacy," The Atlantic, November 1967, at 53.

41. "The New Computer Age," Saturday Review, July 23, 1966, at 15.

42. The Computer and Invasion of Privacy: Hearings Before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations, 89th Cong., 2d Sess. 295 (1966).

43. Rosenberg, The Death of Privacy at 28.

44. "Report of the Committee on the Preservation and Use of Economic Data to the Social Science Research Council" (April 1965), reprinted in House hearings on The Computer and Invasion of Privacy at 195-254, supra note 42.

45. "Statistical Evaluation Report No. 6--Review of the Proposal for a National Data Center," reprinted in House hearings on The Computer and Invasion of Privacy 254-294 (the Dunn Report), supra note 42. Cited in Rosenberg, The Death of Privacy at 32.

46. Rosenberg, The Death of Privacy at 32-33.

47. Id. at 34.

48. "Report on the Task Force on the Storage and Access to Government Statistics" (the Kaysen Report), cited in Rosenberg, The Death of Privacy at 33.

49. The Computer and Invasion of Privacy at 52.

50. Id.

51. Id. at 1.

52. Id. at 2.

53. Id.

54. Id. at 3.

55. Id.

56. Id. at 4.

57. Id.

58. Id. at 6.

59. Id. at 11.

60. Id.

61. Id. at 12.

62. Id. at 25.

63. Id. at 27.

64. Id. at 28.

65. Id. at 50.

66. Id.

67. Id. at 51.

68. Id. at 93.

69. Id. at 92.

70. Id. at 92-93.

71. Id. at 35, 38, reprinting John W. Macy, Jr., "The New Computerized Age--4: Automated Government," Saturday Review, July 23, 1966, at 23.

72. Id. at 38.

73. See generally Invasion of Privacy: Hearings Before the Subcommittee on Administrative Practices and Procedures of the Senate Committee on the Judiciary, 89th Cong., 2d Sess. (1966).

74. Id. at 2388.

75. Id.

76. Id. at 2389-2390.

77. Id. at 2405.

78. See e.g., Computer Privacy: Hearings Before the Subcommittee on Administrative Practices and Procedures of the Senate Committee on the Judiciary, 90th Cong., 1st Sess. (1967).

79. See generally Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 92nd Cong., 1st Sess. (1971).

80. Id. at 6.

81. Id. at 5.

82. Id. at 6.

83. Id. at 1.

84. Id. at 2.

85. Id. at 3.

86. Id. at 2.

87. Id. at 6, quoting Westin, Privacy and Freedom.

88. Id. at 8.

89. Id.

90. Id. at 9.

91. Id. at 11.

92. Id. at 17.

93. Id. at 23.

94. Id. at 27, 37.

95. Id. at 73.

96. Id. at 79.

97. See 120 Cong. Rec. 12646-12650 (daily ed. May 1, 1974), for Senator Ervin's comments when he introduced the Senate version of the privacy bill (S. 3418, 93rd Cong., 2d Sess.). The Senate Government Operations Committee's ad hoc Subcommittee on Privacy and Information Systems held joint hearings with the Senate Judiciary Committee's Subcommittee on Constitutional Rights, which was considering similar legislation. Cited in S.Rep. No. 1183, 93rd Cong., 2d Sess. (1974), reprinted in U.S. Cong. & Admin. News 6918-6919 (1974).

98. U.S. Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens viii (1973).

99. Id. at vii, ix.

100. Id.

101. Id. at vi.

102. Id. at v, vi.

103. Id. at xx, xxi.

104. Administrative data systems contain personal information necessary for the day-to-day operations of agencies. Statistical data systems compile personal information for research purposes and to inform public policy.

105. Records, Computers and the Rights of Citizens at xii.

106. Id.

107. Id. at xxiii.

108. S.Rep. No. 1183 at 6918-6919, supra note 97.

109. Id. at 6919.

110. Id. at 6922.

111. Id.

112. The Privacy Act of 1974, 5 U.S.C. 552a et seq.
113. S.Rep. No. 1183 at 6916.
114. Id. at 6943.
115. See generally Thomas M. Susman, "The Privacy Act and the Freedom of Information Act: Conflict and Resolution," 21 J. Marshall L. Rev. 703 (1988).
116. S.Rep. No. 1183 at 6938. The Privacy Protection Commission was to consist of five experts from specialized fields covering law, social science, computer technology, civil liberties, business, and state and local government.
117. Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment 113 app. 4 (1977).
118. Id. at 113.
119. The Computer and Invasion of Privacy at 120-122.
120. Computer Matching and Privacy Protection Act of 1988, H.Rep. 802, 100th Cong., 1st Sess., reported in U.S. Cong. & Admin. News 3109 (1988).
121. The Privacy Act allows agencies to collect and disseminate personal information pursuant to the agencies' statutory duties and other "routine" uses. See 5 U.S.C. sec. 552a(e)(3). Agencies defined this term loosely, concluding that sharing personal data with other agencies for reasons related to the agencies' statutory roles was "routine" use.
122. H.Rep. No. 802 at 3110.
123. Id. at 3109.
124. See Evan Hendricks, "How Not to Catch Welfare Cheaters," The Washington Post, July 1, 1979, at C8.
125. U.S. Congress Office of Technology Assessment, Computer-Based National Information Systems 75-76 (1981).
126. See generally Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs, 97th Cong., 2d Sess. (1982).
127. Id. at 176.
128. Id. at 129-139.

129. Id.

130. Id. at 117-120.

131. See generally Computer Matching and Privacy Protection Act of 1986: Hearings Before the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs, 99th Cong., 2d Sess. (1986).

132. Id. at 29.

133. U.S. Congress Office of Technology Assessment, Electronic Record Systems and Individual Privacy 46 (1986).

134. See generally Computer Matching and Privacy Protection Act of 1987: Hearings Before the House Committee on Government Operations, 100th Cong., 1st Sess. (1987).

135. Id. at 70.

136. Computer Matching and Privacy Protection Act, Pub.L. No. 100-503, 102 Stat. 2507 (1988).

137. H.Rep. No. 802 at 3108.

138. Fair Credit Reporting Act, 15 U.S.C. sec. 1681 (1976).

139. Id.

140. Leonard Sloane, "One-Stop Credit Report Covers Three Bureaus' Data," The New York Times, July 26, 1992, at 50.

141. Fair Credit Billing Act, 15 U.S.C. sec. 1666 (1976).

142. Family Education Rights and Privacy Act, 20 U.S.C. sec. 1232 (1976).

143. Right to Financial Privacy Act, 12 U.S.C. secs. 3401-3422 (1976).

144. United States v. Miller, 425 U.S. 325 (1976).

145. Id. at 449.

146. Right to Financial Privacy, supra note 144.

147. Computer Crime Act, 18 U.S.C. sec. 1030 (1984), amended by Pub.L. No. 99-473 (1986).

148. Senator Mathias expressed alarm that the Computer Crime Act might be construed to apply even when the Freedom of Information Act required disclosure of information. See 131 Cong. Rec. 2728 (daily ed. March 7, 1985).

149. See generally Susman, "The Privacy Act and the Freedom of Information Act: Conflict and Resolution," supra note 115. Forty-nine states also have computer crime legislation, covering a range of activities. See Robert Ellis Smith, Compilation of State and Federal Privacy Laws 9-11 (1992). For example, California's law makes it a crime to intentionally access " . . . any computer system or computer network for the purpose of devising, or executing any scheme or artifice; to defraud or extort or obtain money, property or services with false or fraudulent intent, representations, or promises; or to maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data." (Cal. Penal Code sec. 502.) Other states with computer crime statutes are: Alabama, Ala. Code 13A-8-101; Arizona, Ariz. Rev. Stat. secs. 13-20301E, 13-2316; Arkansas, Ark. Code Ann. secs. 5-41-103, 5-41-104; Colorado, Colo. Rev. Stat. sec. 18-5.5-101; Connecticut, Conn. Gen. Stat. Ann. sec. 53a-250; Delaware, Del. Code tit. 11, secs. 931-939; Florida, Fla. Stat. Ann. sec. 815.01; Georgia, Ga. Code Ann. sec. 16-9-90; Hawaii, Haw. Rev. Stat. 708-890; Idaho, Idaho Code sec. 18-22; Illinois, Ill. Stat. Ann. ch. 38, para. 16D; Indiana, Ind. Code Ann. secs. 35-43-1-2 through 4; Iowa, Iowa Code Ann. sec. 716A; Kansas, Kans. Stat. Ann. sec. 21-3755; Kentucky, Ky. Rev. Stat. sec. 434.840; Louisiana, La. Rev. Stat. 14:73.1 through 5; Maine, Me. Rev. Stat. Ann. tit. 17A, sec. 431; Maryland, Md. Ann. Code art. 27, sec. 146; Massachusetts, Mass. Gen. Laws Ann. ch. 266, drv 30(2); Michigan, Mich. Comp. Laws Ann. sec. 752.791; Minnesota, Minn. Stat. Ann. 609.89; Mississippi, Miss. Code Ann. sec. 97-45-1; Missouri, Mo. Ann. Stat. sec. 569.093; Montana, Mont. Code Ann. 46-6-310; Nebraska, Neb. Rev. Stat. sec. 28-1343; Nevada, Nev. Rev. Stat. sec. 205.473; New Hampshire, N.H. Rev. Stat. Ann. sec. 638:16; New Jersey, N.J. Rev. Stat. secs. 2A:38A-1, 2C:20-1; New Mexico, N.M. Stat. Ann. sec. 30-16A-1; New York, N.Y. Penal Law para. 156; North Carolina, N.C. Gen. Stat. 14-453; North Dakota, N.D. Cent. Code sec. 12.1-06.1-08; Ohio, Ohio Rev. Code Ann. secs. 2901.01 and 2913.01; Oklahoma, Okla. Stat. Ann. tit. 21, secs. 1951-1956; Oregon, Or. Rev. Stat. 164.377; Pennsylvania, Pa. Stat. Ann. tit. 18, sec. 3933; Rhode Island, R.I. Gen. Laws sec. 11-52-1; South Carolina, S.C. Code sec. 16-16-10; South Dakota, S.D. Codified Laws Ann. sec. 43-43B-7; Tennessee, Tenn. Code Ann. sec. 39-14-60; Texas, Tex. Penal code Ann. sec. 33.01; Utah, Utah Code Ann. sec. 76-6-701; Virginia, Va. Code sec. 18.2- 152.1; Washington, Wash. Rev. Code Ann. sec. 9A.48.100; West

Virginia, W.Va. Code sec. 61-3c-4 through 12; Wisconsin, Wis. Stat. Ann. sec. 943.70; Wyoming, Wyo. Stat. sec. 6-3-501 through 504.

150. Electronic Communications Privacy Act of 1986, 18 U.S.C. sec. 2510 (1986). See S.Rep. No. 541, 99th Cong., 2d Sess. (1986), reprinted in U.S. Code Cong. & Admin. News 3555 (1986).

151. Id.

152. Computer Security Act of 1987, Pub.L. No. 100-235.

153. H.Rep. No. 153, 100th Cong., 1st Sess. (1987), reprinted in U.S. Code Cong. & Admin. News 3139 (1987).

154. Id. at 3138.

155. Id. at 3133.

156. Id.

157. Id.

158. Id. at 3182.

159. The Video Privacy Protection Act grew out of the outrage of many U.S. Senators over the intrusion into the Bork family's privacy. See Nomination of Robert H. Bork to be Associate Justice of the Supreme Court of the United States: Hearings Before the Senate Committee on the Judiciary, 100th Cong., 1st Sess., 1374 (1987) (remarks of Sen. Patrick Leahy, D-VT).

160. In 1986, twenty years after the Freedom of Information Act was passed, the federal government operated about 22,000 mainframe computers; by 1990, that number more than doubled to 48,000. See General Service Administration, Federal Equipment Data Center, Automated Data Processing Equipment in the U.S. Government (April 1990).

CHAPTER FOUR
COURT CASES ADDRESSING PRIVACY CONCERNS
ABOUT COMPUTERS

A Question of Balance

Chapter Two tracked the development of social values and legal theories supporting the concept of personal privacy. In addition, it followed the development of social and political values underlying the theory that the public, to maximize the benefits of a self-governed, democratic society, should have access to government information unless the government had an important reason not to disclose specific information. The chapter, along with discussion of legislative responses to privacy concerns in Chapter Three, explored the potential conflict between personal privacy and access to government records and suggested the following question: At what point do computer privacy concerns constitute a sufficient justification for the government to withhold information from the public?

This chapter explores how courts have attempted to resolve privacy-related issues that have arisen because information was held in government computers. Conflicts have occurred for at least three reasons, which were outlined in Chapter One. They are mechanical and

technological problems, interpretational or definitional problems, and public policy questions.

Mechanical and technological problems related to privacy have occurred simply because the computer machinery, or hardware, stands between the record requester and record custodian. Requesters frequently do not know the proper questions to ask to obtain disclosable information. On the other hand, record custodians may not be properly trained or are indifferent to the technology and, therefore, are unresponsive to legitimate access requests.

Interpretational and definitional problems occur because most records-access laws predate the widespread use of computers by government. Issues settled at a time when most records were in paper form have become muddled when those same records are held in government computers. When records were computerized, agencies no longer were clear on what constituted a reasonable response when information was contained in data base.

Public policy questions have arisen on a number of fronts. One involves costs. How much time and energy must agencies expend to use computer technology to provide reasonable access? At what point should costs, such as reprogramming computers or undertaking extensive data base searches, give way to the public interest in limiting or reducing government expenditures?

Another--more problematic--public policy question involves the very nature of computers and their potential impact on society. This issue was played out on the legislative stage during the 1960s in debates over the proposal for a National Data Center, discussed at length in Chapter Three. Fear about the threat of computers to personal privacy during the National Data Center controversy and in subsequent hearings led to legislative conclusions that computers exacerbated privacy dangers and their use should be restrained. The result was passage of the Privacy Act of 1974 and other computer-related legislation that placed limits on government information practices, all of which were discussed in Chapter Three.

The important public policy concern about the very role of computers in a democratic society was at the heart of a 1989 U.S. Supreme Court opinion, United States Department of Justice v. Reporters Committee for Freedom of the Press, which the U.S. Department of Justice has referred to as a "landmark" case in public access law.¹ In the opinion, the Court attempted to strike a balance between the Judeo-Christian concept of "forgive and forget" and the public interest in access to personal or otherwise private criminal-history information held in government computers--information that existed somewhere at some time in public records. The computer, the Court reasoned, robbed individuals of "practical obscurity," or the natural

barriers of time and distance that protected individuals from routine accumulation of information about them. These computer-privacy issues are addressed in the next few pages, beginning with cases that deal with the broader public policy issues and broach the question of a constitutional right of informational privacy. Subsequent discussion deals with privacy cases related to technical and definitional questions raised when records are held in government computers. Analysis focuses on federal cases but also looks at how state courts have dealt with related issues.

A Right of Informational Privacy?

A right of privacy is mentioned nowhere in the U.S. Constitution or any of its amendments. However, as the previous discussion of development of privacy as a social value and legal concept shows, privacy rights are recognized in the common law² and in legislation,³ and the U.S. Supreme Court has fashioned constitutional protections in some areas. The Court has recognized a right of privacy within one's home⁴ and within other "zones" of privacy not dependent on a specific location,⁵ as well as associational privacy, preventing government interference in private associations and political affiliations.⁶ The Court also has recognized a right of decisional privacy, preventing interference in intimate, personal decisions such as the use of birth control⁷ and abortions.⁸

More recently, the Court also has recognized government has a duty to ensure that private information it collects and stores in computers is protected from unwarranted disclosure⁹ and that individuals have a right to control how private information about themselves is used and disseminated.¹⁰ Whether this concept of informational privacy rises to the same constitutional stature of other core privacy rights gleaned from the Constitution and Bill of Rights by the Court remains to be seen.

The following discussion explores court cases that have helped define the dimensions of informational privacy. Concerns about computers and privacy expressed in congressional hearings during the 1960s and early 1970s that led to passage of the Privacy Act of 1974 and other legislation echo throughout many of the cases.

The Seeds of Informational Privacy

The notion that individuals should control private information about themselves predates the American Revolution, both in the English common law that provided the historical foundation for the American legal system and in the colonial experience of this nation. For example, in Pope v. Curl, an English court using a property rights analysis held that individuals should control dissemination of their private matters, in this case the content of personal letters.¹¹ In the American colonial period, when Ben Franklin was postmaster general, regulations required

postmasters to take an oath to ensure the privacy of the mails.¹² The common law also recognized that individuals had an interest in controlling information about themselves, but this interest was mitigated when the information was a matter of public concern.¹³ But with the social and technological changes in the last half of the twentieth century and the accompanying information revolution, the ability of individuals to control information about themselves has eroded substantially. This lack of control is the result of the sheer volume of personal information flowing in American society, coupled with statutory and administrative safeguards that have not kept pace with social and technological changes.¹⁴ As a result, laws meant to ensure privacy as well as those designed to ensure access to government information have become less effective in resolving privacy-access conflicts.

The Supreme Court and Informational Privacy

The initial reluctance of the Supreme Court to fully embrace the concept of informational privacy is illustrated in a pair of 1976 cases. In Paul v. Davis, a man against whom shoplifting charges were filed but later dismissed sought relief after police in Louisville, Kentucky, included his name in a listing of "active shoplifters" distributed to 800 local merchants.¹⁵ On a 5-3 vote, the Court refused to expand constitutional privacy to cover the dissemination by police of such personal and defamatory information. Justice

Rehnquist, who would later sit as chief justice, balked at the notion of a constitutional basis for informational privacy. He distinguished privacy interests in the control of personal information from privacy cases that dealt with substantive restrictions on activities such as contraception and procreation. "None of our substantive privacy decisions hold this or anything like this, and we decline to enlarge them in this manner," Justice Rehnquist wrote.¹⁶

In United States v. Miller, decided soon after Paul, the Court again declined to recognize a right of informational privacy in a case that dealt with a man's control of personal information he provided to a bank.¹⁷ The Fourth Amendment case, decided on a 5-4 vote, addressed privacy interests in information given to third parties, not to the government. Because the government was not a party to the information gathering and dissemination in the case, the activities of the bank did not pose a direct constitutional question. The case did, however, provide additional insight into the informational privacy issue and, in a dissenting opinion by Justice Brennan, reflect a growing concern among some members of the Court about the special dangers new information technology posed to privacy.

The Miller case began when the government sought banking records related to a criminal investigation. The bank, which had not been served a search warrant, voluntarily provided the records. The subject of the

records challenged the government, maintaining he had been deprived of legal due process because the records were obtained by the government without a search warrant. To resolve the issue, the Court applied a "reasonable expectation of privacy" standard articulated by the Court in the 1967 case Katz v. United States.¹⁸ In Katz, the Court held that the Fourth Amendment protected individuals from warrantless wiretaps, even if calls were monitored in telephone booths, not their homes. The Court reasoned that the Fourth Amendment protects individuals, not places, and that in American society people enjoy a "reasonable expectation of privacy" in places outside the home. The Katz holding also suggested that constitutional protections extend not only to personal property, but also to personal communications and information contained in them.

The Miller Court, however, reasoned that when individuals voluntarily turn records over to banks, the records become the property of the banks; consequently, the individuals relinquish any reasonable expectation of privacy with respect to those records.¹⁹ Although the case was decided against the person on whom records were kept, it did reflect a nagging concern among some members of the Court about privacy problems that lay ahead because of computers and the proliferation of personal information in American society. In dissent, Justice Brennan echoed the sentiments of John Adams, cited in Chapter One, that there is some

information about individuals that "others have not a Right to Know."²⁰ Justice Brennan said,

A bank customer's reasonable expectation is that, absent a compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. . . . [An individual] reveals many aspects of his personal affairs, opinions, habits, associations. Indeed, the totality of bank records provides a virtual current biography. Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the constitutional protection must keep pace with the perils created by these new devices.²¹ (Emphasis added)

The threat of unchecked disclosure of banking records to the privacy of individuals was not lost on Congress, which not long before the Miller opinion had held extensive hearings into the computer-privacy issue that ultimately led to passage of the Privacy Act of 1974.²² Responding to the Court's ruling in Miller, Congress passed the Right to Financial Privacy Act. The Right to Financial Privacy Act, discussed in Chapter Three, includes due process standards and requires law enforcement agencies to meet certain criteria before banking records may be released.²³

A year after Miller, the Court for the first time considered a case that dealt squarely with computerized records maintained by government. In Whalen v. Roe, the concerns about technology and personal privacy expressed in Justice Brennan's dissent in Miller were embraced by a majority on the Court.²⁴ The opinion in Whalen nudged the

concept of informational privacy near, if not into, the constitutional realm.

In Whalen, several physicians and patients challenged the constitutionality of a New York statute that required doctors to provide the state with copies of prescriptions for certain kinds of controlled drugs, to be maintained in a state computer system. The purpose of the program was to monitor the dispensing of the controlled drugs. It was enacted as the Controlled Substance Act of 1972 by the New York Legislature in response to concerns that controlled drugs were being diverted into unlawful channels.²⁵ The doctors argued that the drug-monitoring system interfered with their ability to practice medicine free from government interference; the patients argued that the statute discouraged them from seeking needed medications. Both assertions were based on concerns that the state's computerized record system might be abused if improperly administered, resulting in violations of privacy interests. A federal district court ruled that the New York statute was an unconstitutional violation of protected rights of privacy and enjoined its enforcement.²⁶ The state appealed and the U.S. Supreme Court agreed to hear the case.

The Supreme Court reversed the lower court and said the statute was a reasonable exercise of the state's broad police powers, that the plaintiff's concerns about the

security of the state's computer system were speculative and not supported by facts presented in the case.²⁷

Justice Stevens, writing for the seven-member majority, posed the legal issue before the Court in constitutional terms. He said the "constitutional question presented is whether the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and unlawful market."²⁸

In his analysis of the case, Justice Stevens recognized two kinds of constitutional privacy interests asserted by the patients and doctors. The first was in informational privacy, or the interest of individuals in avoiding disclosure of personal matters.²⁹ The second interest was decisional privacy, or independence in making certain kinds of personal decisions.³⁰ Although Justice Stevens recognized two such interests, he said insufficient evidence was presented to suggest the New York program violated either. With respect to the informational privacy claim, he noted that public disclosure of patient information could occur in three ways: Health department employees might violate the statute, either deliberately or negligently, that required them to maintain proper security; a patient or doctor might be accused of a crime and the computerized data taken as evidence in a criminal proceeding; or a doctor, pharmacist,

or patient might voluntarily make the information public. He concluded that the third possibility existed under prior law and was totally unrelated to the computer-filing program and that neither of the first two concerns was sufficient to render the statute invalid. With respect to the computer security issue, Justice Stevens noted there was no support in the record, or in the experience of two states with similar statutes,³¹ to suggest New York's program would likely be administered improperly.³²

While the Court held that New York's computer-based program for monitoring controlled drugs did not violate a constitutional right of individuals to control private information about themselves, the opinion expressed concerns about the impact of computers. Justice Stevens offered a "final word about issues we have not decided" in the opinion, which echoed many of the concerns expressed in the legislative debates of the previous decade about computer privacy.³³ He also provided a constitutional footing for those concerns. Addressing what he viewed as potential constitutional pitfalls as society grew increasingly dependent on computers, he observed,

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and

use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosure. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.³⁴

The ruling did provide some guidance about how the Court might deal with computer privacy and access conflicts in future cases. While the Court recognized the privacy interests of individuals in personal information, it also recognized that reasonable computer security precautions by administrative agencies were sufficient to ensure privacy. In other words, properly administered computerized record systems could be made as secure from unauthorized access as paper record systems. Taking this reasoning a step further, the opinion rejected the notion that the mere fact records were held in computers could justify for blanket denial of public access to all records in the computer. This recognition by the Court is important because it undermines potential agency arguments that access to computerized records should be curtailed simply because of speculative privacy dangers or because of concerns based on generalized fears of computer technology.

Justice Brennan, concurring in the result in Whalen, also expressed concerns about the effects of computer technology on personal liberties. He conceded that government had a legitimate interest in the collection and storage of personal data in computers and that simply because new technology made government more efficient was not reason enough to render such activities unconstitutional. But he cautioned that broad dissemination of such private information would "clearly implicate constitutionally protected privacy rights."³⁵ In words that anticipated Court actions, Justice Brennan said,

The Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increases the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curbs on such technology.³⁶

A dozen years after Whalen, developments in government use of computer technology brought the issue squarely back before the Court in United States Department of Justice v. Reporters Committee for Freedom of Information, a case that could significantly reduce public access to government information held in centralized computers.³⁷

A Seminal Case for Informational Privacy

In 1989, the Supreme Court decided a case that had lingered in the federal courts for more than a decade. In United States Department of Justice v. Reporters Committee,³⁸ the Court arguably recognized a constitutional right of

informational privacy on a par with other privacy interests acknowledged by the Court.

The unanimous opinion by Justice Stevens in Reporters Committee has important implications for access to computerized records on several fronts. First, the Court adopted a legal definition of privacy that recognized the rights of individuals to control personal information about themselves--even information about criminal arrests and convictions that existed in public records somewhere and in many cases was accessible under the common law.

Second, the Court articulated a "practical obscurity" doctrine, a judicial acceptance of, among other things, the adage "forgive and forget." The Court's practical obscurity doctrine assumes that computers exacerbate the threat to personal privacy by eliminating the natural elements of time and distance among "scattered bits of information" that once afforded individuals the ability to distance themselves from past mistakes and start their lives anew. The doctrine also assumes that scattered bits of information about an individual, when pieced together in a computer, create a composite that is more threatening than any separate bit of information. As a result, information--even information compiled from scattered public records--gains a revitalized privacy interest when pooled in a centralized computer system, the Court reasoned.

Third, the Court said agencies could determine that classes of information--in this case compilations of public record information in computerized data bases--could be "categorically" recognized as an unacceptable privacy threat and shielded from public disclosure without any meaningful balancing with competing societal interests, such as a public interest served by disclosure.

This is similar to "sensitive" information that some proponents of an intermediate designation for nonclassified, computerized public information argued should be shielded from routine disclosure. In response to such efforts, Congress had passed the Computer Security Act of 1987, which rejected such a limitation of disclosure.³⁹ The Computer Security Act was discussed in Chapter Three.

Last, the Court said the sole purpose of disclosure under the FOIA was to shed light on the performance of agencies' statutory duties. This definition greatly narrows the scope of public interests that could overcome privacy concerns in access cases and threatens to take out of the public realm vast amounts of information the government gathers and stores in computers that has no obvious bearing on agency performance. The reasoning assumes a public interest in disclosure of specific information only after an agency attempts to draw conclusions or make decisions based on the information. Such reasoning threatens to diminish the watchdog role of the media, other institutions, and

individuals by preventing independent discussion and analysis of information that very well could reflect on an agency's performance but can only be know to do so after analysis. In other words, it prevents independent sources from possibly criticizing an agency not only for what it did do, but also for what it did not. This reasoning also underscores the problem of defining a "record" in the computer age; much of the information government gathers and stores is bulk in nature and does not resemble the traditional reports, memoranda, and other documents that once comprised the contents of agency file cabinets and "shed light" on agency performance.⁴⁰

The facts and legal arguments in the Reporters Committee case, along with its implications for public access to computerized records, are discussed below.

The Long Road to the Supreme Court

The case began in 1978 when CBS news correspondent Robert Schakne and the Reporters Committee for Freedom of the Press filed a Freedom of Information request with the Justice Department for criminal records about four members of the Medico family. The request sought Federal Bureau of Investigation records about arrests, indictments, convictions, sentences, and acquittals. The Pennsylvania Crime Commission had identified the family company, Medico Industries, as a legitimate business dominated by organized crime figures. In addition, the firm allegedly had

improperly received various defense contracts with the aid of a corrupt congressman.⁴¹

The FBI initially denied all of the requests but provided the information on three of the Medico brothers after their deaths in accordance with the agency's disclosure policies. The FBI continued to withhold any records it might have on the remaining brother, Charles Medico, and CBS and the Reporters Committee filed a federal FOIA suit asking a federal district court to compel disclosure. The suit sought disclosure of records on Charles Medico that "were matters of public record."⁴² In a motion for summary judgment, CBS and the Reporters Committee asked for any records "of bribery, embezzlement or other financial crime" that would be a matter of public interest.⁴³ In response to the summary judgment motion, the Justice Department said its files contained no record of financial crimes by Charles Medico but would neither confirm nor deny it had any records related to other crimes.⁴⁴ As a result of the motions, the focus of the CBS and Reporters Committee request was narrowed to nonfinancial crimes that were matters of public record.

The district court held in favor of the Justice Department and based its reasoning on three grounds.⁴⁵ First, the court said the requested information was governed by a statute that allowed sharing of criminal-record information among official agencies but prohibited release

to the general public.⁴⁶ The court, therefore, concluded this information was covered by Exemption 3 of the Freedom of Information Act, which shielded from disclosure information covered by specific statutes. Two requirements must be met for a statute to qualify under Exemption 3: The statute must allow an agency no discretion about what information may be withheld, and the criteria for withholding specific information must be clearly spelled out.⁴⁷ This position--that the information was covered by Exemption 3--was central to the Justice Department arguments in the case.

Second, the court said the requested information was also shielded by Exemption 6 of the FOIA, which covered "personnel and medical files and similar files the disclosure of which would constitute an unwarranted invasion of privacy."⁴⁸ The court said criminal files fell within the "similar files" definition because they were "personal to the individual named therein."⁴⁹ Acknowledging the personal nature of the criminal records, the court proceeded to balance the privacy interest and public interest, concluding disclosure would result in a "clearly unwarranted" invasion of privacy.⁵⁰ Said the court,

It seems highly unlikely that information about offenses which may have occurred 30 or 40 years ago, as in the case of William Medico, would have any relevance or public interest. The same can be said for information relating to the arrest or conviction of persons for minor criminal offenses or offenses which are completely unrelated to anything now under consideration by

the plaintiffs. That information is personal to the third party (Charles Medico), and it if [sic] exists, its release would constitute "a clearly unwarranted invasion of personal privacy."⁵¹

The third reason the court gave was that the criminal records were also covered by Exemption 7(C) of the FOIA, which dealt specifically with privacy interests in criminal history records. After viewing the records privately, the court sealed them and said it would not reconsider the matter.⁵²

CBS and the Reporters Committee appealed, and the Court of Appeals for the District of Columbia Circuit reversed the lower court.⁵³ In its initial ruling, the Court of Appeals held that the criminal-records nondisclosure statute did not qualify as an Exemption 3 statute under the FOIA and that the lower court had misapplied Exemptions 6 and 7(C). The court concluded that individual privacy interests were at best minimal in criminal history information that was a matter of public record--even if those records were compiled in a large national data bank. The D.C. Circuit conceded that maintaining the obscurity of computerized criminal records was "attractive as a legislative policy matter" but was not related to the statutory meaning of privacy in this context.⁵⁴

Absent a statutory definition of public interest in disclosure, the court reasoned, it should follow the practices of state and local governments. The court had been advised that most state and local governments made

criminal records available to the general public.⁵⁵ If local governments disclosed such information to the public, these policies were evidence of a public interest in disclosure, the court reasoned. Finding only a minimal privacy interest in publicly available criminal records that was overcome by evidence of a public interest in disclosure, the court remanded the case to the district court with instructions to revise its holding accordingly.⁵⁶

The Justice Department petitioned for a rehearing and advised the appellate court that criminal-history records were not, in fact, widely available to the public at the state and local level. The Justice Department included a brief by Search Group, Inc., an association of state and local law enforcement officials. The brief, among other things, stated that criminal records at the state and local levels were not as available as the D.C. Circuit had been led to believe.⁵⁷

The D.C. Circuit denied the petition for rehearing but modified its earlier ruling regarding the balancing of privacy concerns and the public interest in disclosure.⁵⁸ The court maintained its view that there was little or no privacy interest in information that already was a matter of public record. However, the court abandoned its reliance on state and local practices as evidence of a public interest in disclosure. The court concluded it was not in a position to reasonably assess the public interest in any particular

government record; instead, the court reasoned that the only public interest to be considered in Exemption 6 and 7(C) cases was the general disclosure policy of the FOIA. "We do not believe that the phrase 'public interest' as used in the balancing in Exemptions 6 and 7(C) of the Act means anything more or less than the general disclosure policies of the statute."⁵⁹

The court further reasoned that since Congress had provided no standard for assessing the public interest in disclosure of information in the FOIA, it did not intend for the judiciary to construct a hierarchy for judging public interest in the disclosure of any particular information. The court conceded the Supreme Court required that courts balance privacy interests with the public interest in Exemption 6 and 7(C) cases to determine whether disclosure might be warranted.⁶⁰ But, the court concluded "that we must balance the prospective damage to the privacy interest against the public's interest does not necessarily mean, we concluded, could not mean, that the public interest depends on our appraisal of the public's need to know particular information."⁶¹

The Justice Department petitioned the U.S. Supreme Court for a writ of certiorari, abandoning entirely its claim that the criminal-record nondisclosure statute qualified under the FOIA's Exemption 3. Instead, the Justice Department argued that Exemptions 6 and 7(C) cases

required a case-by-case balancing of privacy and the public interest with respect to the specific information sought.

In its petition, the Justice Department lambasted the D.C. Circuit:

The court of appeals chose to use this case as a vehicle to rewrite the FOIA law. . . . These novel principles conflict with prior decisions of [the Supreme Court] and other courts of appeals, and they constitute an advertent attempt to make important new law. . . . The principles announced by the court of appeals flout the intent of Congress that the courts engage in meaningful balancing in Exemption 6 and 7(C) cases.⁶²

The Supreme Court granted certiorari⁶³ and issued its opinion on March 22, 1989.⁶⁴ Justice Stevens wrote the majority opinion, joined by Justices White, Marshall, O'Connor, Scalia, Kennedy, and Chief Justice Rehnquist. Justice Blackmun, joined by Justice Brennan, filed an opinion concurring with the result.⁶⁵

A Definition of Informational Privacy

Justice Stevens, in beginning his analysis, noted that the Court agreed to hear the case because of its potential impact on "values of personal privacy."⁶⁶ While the case involved the statutory interpretation of a FOIA exemption, he posed the legal question before the Court in broader, constitutional terms. Citing his earlier opinion in Whalen v. Roe, Justice Stevens noted that privacy cases have asserted two constitutional values: the interest in avoiding disclosure of personal information and independence in making certain kinds of intimate decisions. "Here, the

former interest 'in avoiding disclosure of personal matters' is implicated," he said.⁶⁷

Justice Stevens promptly rejected as a "cramped notion of personal privacy" the assertion that criminal-record information had no privacy interest because it had previously been disclosed publicly.⁶⁸ Ignoring the fact people generally have no control over disclosure of criminal records,⁶⁹ he noted that both the common law and the literal understanding of privacy acknowledge the right of individuals to control information about themselves. To bolster this reasoning, Justice Stevens cited Webster's Dictionary⁷⁰ as well as legal commentators, including Alan Westin, whose book Privacy and Freedom and congressional testimony influenced the public policy debate over privacy and the computerization of government records. As Westin defined it, "Privacy is the claim of individuals . . . to determine for themselves when, how and to what extent information about them is communicated to others."⁷¹ Justice Stevens also cited the seminal 1890 article in the Harvard Law Review by Samuel Warren and Louis Brandeis, who would later sit on the Supreme Court, that said,

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. . . . [E]ven if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.⁷²

A Public Record in the Computer Age

After adopting a definition of informational privacy that encompassed at least some publicly available government records, Justice Stevens set about to distinguish between public and private information. He offered a definition of public records that turned not on the nature of the records but on the nature of the system in which the records were kept and the difficulty of obtaining them. He reasoned that if the records sought by CBS and the Reporters Committee were truly "public," an FOIA request would not have been necessary. Said Justice Stevens,

The very fact that federal funds have been spent to prepare, index, and maintain these criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be "freely available" either to the officials who have access to the underlying files or to the general public. Indeed, if the summaries were "freely available," there would be no reason to invoke the FOIA to obtain information they contain. Granted, in many contexts the fact that information is not freely available is no reason to exempt that information from a statute generally requiring its dissemination. But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.⁷³ (Emphasis added)

Justice Stevens cited several statutes and regulations to support the Court's conclusion that records that were public somewhere or at some time in government record

systems could nonetheless be shielded from disclosure when compiled in government computers. He noted that Congress limited criminal record dissemination to banks, the securities industry, the nuclear power industry, law enforcement agencies, and local licensing agencies.⁷⁴ He also cited an FBI program that disseminated criminal-history records to law enforcement agencies but that threatened to terminate the sharing if the information were disclosed "outside the receiving departments or related agencies."⁷⁵

To further support the Court's position, Justice Stevens cited the Privacy Act of 1974, which recognized "the impact of computer data banks on individual privacy."⁷⁶ Justice Stevens said the Privacy Act could not be used to withhold information required to be disclosed under the FOIA, a conclusion Congress itself had reached in 1984.⁷⁷ But he ignored Congress' specific prohibition against using the Privacy Act to withhold public-record information and surmised that "Congress' basic policy concern regarding the implications of computerized data banks for personal privacy is certainly relevant in our consideration of privacy interests affected by dissemination of rap sheets from the FBI computer."⁷⁸

Justice Stevens cited two examples in the FOIA itself to bolster his conclusion that Congress had not intended the disclosure statute to cover records of private citizens, identifiable by name. He pointed out that the FOIA

specifically provides that "[to] the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instructions."⁷⁹ He added that the FOIA required that "[any] reasonably segregable portion of a record shall be provided . . . after deletion of the portions which are exempt."⁸⁰ This requirement, he reasoned, was an acknowledgement by Congress that disclosure of records containing personal information about private citizens could infringe on significant privacy interests.⁸¹

In an additional attempt to distinguish between "scattered bits of criminal history and a federal compilation,"⁸² Justice Stevens referred to the Court's opinion in Department of Air Force v. Rose, a case that recognized privacy interests in cadet disciplinary reports that at one time had been posted on bulletin boards at the United States Air Force Academy, a military educational institution not routinely open to the public.⁸³

Rose began when New York University law students writing about military discipline sought summaries of Air Force Academy Honor and Ethics Code violations. The law students sought only summaries with "personal references and other identifying information deleted."⁸⁴ The Rose Court held, however, that what constitutes identifying information must be weighed not only from the viewpoint of the general

public but also from the perspective of other cadets and academy personnel who might recognize the subjects of the disciplinary actions. Justice Stevens, equating public criminal records to institutional disciplinary records, seemed to suggest that records could endanger privacy and be withheld based on a very limited, speculative threat. He noted,

If a cadet has a privacy interest in past discipline that was once public but may have been 'wholly forgotten,' the ordinary citizen surely has a similar interest in the aspects of his or her criminal history that may have been wholly forgotten."⁸⁵

Citing his earlier opinion in Whalen, Justice Stevens made clear in Reporters Committee that "wholly forgotten" criminal records regained privacy interests when compiled by government computers: "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks."⁸⁶ To underscore the Court's concern about computers and the dimensions of informational privacy, Justice Stevens cited a lecture by Chief Justice Rehnquist, who had written the majority opinion in Paul v. Davis that rejected a constitutional right of informational privacy. The chief justice noted that the fact "an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."⁸⁷

Purpose of Disclosure

Next, Justice Stevens turned to the question of the purpose of disclosure. CBS and the Reporters Committee had argued there were two issues related to Charles Medico's possible criminal history that supported a public interest in disclosure: Medico allegedly had improper dealings with a corrupt congressman, and Medico also was a principal in a corporation that received contracts from the Department of Defense. Justice Stevens rejected this kind of a public interest argument, accepted by several lower courts, that a court should look at the purpose of disclosure when balancing privacy interests with the public interest served by disclosure. He said that if Medico had, in fact, been arrested or convicted of certain crimes, that information would "neither aggravate nor mitigate his alleged improper relationship with the Congressman. . . [and] tell us nothing directly about the character of the Congressman's behavior."⁸⁸ Likewise, Justice Stevens said that such information would not "tell us anything about the conduct of the Department of Defense (DOD) in awarding one or more contracts to the Medico Company."⁸⁹

Instead of looking at the public interest side of the balancing equation in terms of the societal benefits that might accrue from disclosure, Justice Stevens said disclosure "must turn on the nature of the requested document and its relationship to the basic purpose of the

Freedom of Information Act."⁹⁰ This primary purpose of the FOIA, he concluded, was "to open agency action to the light of public scrutiny,"⁹¹ not to provide access to information for reasons that might have some secondary benefit to society. He also noted that Congress had recognized this kind of public interest when it established a fee structure for providing documents under the FOIA. The FOIA provides for fee waivers or reduced fees "if disclosure of the information is in the public interest because it contributes significantly to public understanding of the operations and activities of government."⁹² Justice Stevens conceded there was "some public interest in providing interested citizens with answers to their questions about Medico." But he said that interest "falls outside the ambit of the public interest that the FOIA was enacted to serve."⁹³ Regarding the purpose of access, Justice Stevens concluded,

Official information that sheds light on an agency's performance of its statutory duties falls squarely within the statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct. In this case . . . the requester does not intend to discover anything about the conduct of the agency that has possession of the requested records. Indeed, response to this request would not shield any light on the conduct of any Government agency or official.⁹⁴

The definition of public interest that Justice Stevens articulated departs from the reasoning in several earlier FOIA cases decided by lower federal courts that weighed

benefits to the public at large from the disclosure of personal information. Some cases looked at the purpose for which the information was requested, inasmuch as the purpose had a direct bearing on how release of information might serve the public interest.

Before Reporters Committee, several courts reasoned that a general public interest was not served in cases where information was sought that would benefit only the requester. Implicit in the reasoning of these cases was that disclosure of information that benefited more than the requester might be in the public interest. In Brown v. FBI, for instance, a court held that it is "the interest of the general public, not that of the private litigant, that must be considered" in balancing the public interest with privacy concerns.⁹⁵ A federal district court followed similar reasoning in Lloyd & Henniger v. Marshall, which said persons who seek records for personal lawsuits do not further a public interest.⁹⁶

Courts also have held that information sought for strictly commercial purposes serves little or no public interest. In Multnomah County Medical Society v. Scott, the Ninth Circuit of the U.S. Court of Appeals held that a requester's commercial interest in the names and addresses of Medicare recipients failed to "warrant disclosure of otherwise private information."⁹⁷ In another Ninth Circuit case, Minnis v. Department of Agriculture, the court

recognized a legitimate public interest in an agency lottery practice for allocating permits to raft down a federally controlled river. The court, however, rejected the request. It noted that the requester's purpose for seeking the names and addresses of lottery applicants was commercially motivated.⁹⁸ The Third Circuit of the U.S. Court of Appeals reached a similar result in Wine Hobby USA, Inc. v. IRS, a case involving requests for addresses of amateur winemakers. The court held that the request was for commercial purposes and therefore failed to advance a general public interest.⁹⁹

The federal courts have recognized the strongest public interest in disclosure in FOIA cases that provided oversight of government operations. This rationale is similar to the Supreme Court's reasoning in Reporters Committee, although several lower courts have been willing to look beyond only that which reflects on an agency's statutory duties. An example of a court's willingness to go beyond scrutiny of an agency's actions is Columbia Packing Co. v. United States Department of Agriculture.¹⁰⁰ In this case, involving the identity of inspectors convicted of accepting bribes in a widespread scandal in the meat processing industry, the First Circuit of the U.S. Court of Appeals allowed release of the names, recognizing that to do so might "forestall similar occurrences." The focus of the analysis was not on agency behavior, per se, but rather on a positive future benefit from disclosure. The court noted

Ordinarily the individual careers of public servants would be of small general interest, but the scandal in which Columbia and the inspectors participated was far-reaching and of great notoriety. To forestall similar occurrences, the public has an interest in discerning how the officials conducted themselves prior to their discharge for bribery, how well they were supervised, and whether the USDA or any of its other personnel were chargeable with any degree of culpability for their crimes. . . . While it cannot be known to what extent disclosure of documents to Columbia for use in this administrative proceeding will actually so inform the public at large . . . we conclude that there is a relevant public interest to produce at least some of the documents.¹⁰¹

In Cochran v. United States, the Eleventh Circuit of the U.S. Court of Appeals rejected the privacy claim of an Army general disciplined for the misuse of government facilities; the rejection was based on the deterrent effect of such a disclosure and its newsworthiness.¹⁰² The general had sued the Army for damages, claiming an Army-issued press release disclosing that he had been reprimanded and fined was a "clearly unwarranted invasion of privacy" that violated the Privacy Act. The court, in balancing the general's privacy interests with the public interest in disclosure, concluded that the Army press release contained exactly the kind of information the FOIA directed agencies to disclose. " [T]o forestall future abuses, the public has an interest in any deterrent effect disclosure might have."¹⁰³ The court added, "The legislative history of the [Privacy] Act does not evidence any intent to prevent the disclosure by the government to the press of current,

newsworthy information of importance and interest to a large number of people."¹⁰⁴ Similarly, in International Board of Electrical Workers No. 5 v. Department of Housing and Urban Development, the Third Circuit reasoned the release of the names and addresses of people employed under a federal employment law served the public interest if such release made it more likely contractors, after being publicly identified, would abide by the terms of the law.¹⁰⁵

Categorical Exemption of Information

Before Reporters Committee, federal courts had routinely attempted to balance privacy concerns with the public interest in disclosure on a case-by-case basis. In fact, in NLRB v. Sears, Roebuck & Co., the Supreme Court rejected an argument by the general counsel of the National Labor Relations Board for categorical balancing in an Exemption 7 case involving investigatory records.¹⁰⁶ In rejecting categorical exemptions, the Court cited congressional concern about several federal cases that had allowed categorical exemption of investigatory files under Exemption 7. This concern was reflected in the 1974 amendments to the FOIA that clarified the need for balancing. In NLRB, the Court noted, "The legislative history clearly indicates that Congress disapproves of those cases, relied on by the [NLRB's] General Counsel . . . which relieve the Government of the obligation to show that disclosure of a particular investigatory file would

contravene the purpose of Exemption 7."¹⁰⁷ The Justice Department also argued against categorical exemptions when the U.S. Court of Appeals for the District of Columbia Circuit in Reporters Committee said, categorically, that individuals had no significant privacy interests in information compiled from public records. The Justice Department suggested that the D.C. Circuit "chose to use this case as a vehicle to rewrite the FOIA law."¹⁰⁸

In Reporters Committee, Justice Stevens took a different view of the case-by-case balancing requirement. He agreed with both parties in the case that when privacy and access were in conflict, a case-by-case assessment was necessary. He based his reasoning on the general requirement that courts "shall determine such matters de novo" and on the specific reference to "unwarranted" invasions of privacy in Exemption 7(C), which contemplated a determination of whether a privacy violation might be warranted.¹⁰⁹ But Justice Stevens concluded that meaningful balancing could be achieved without looking at the individual circumstances of a case. Citing the majority opinion by the D.C. Circuit that judges had been given no standards with which to determine a public interest in FOIA cases, he said courts could engage in categorical balancing. "Our cases provide support for the proposition that categorical decisions may be appropriate and individual circumstances disregarded when a case fits into a genus in

which the balance characteristically tips in one direction."¹¹⁰ Computer compilations of criminal records--even information taken only from public records--could be categorically excluded from disclosure because they "characteristically" tip toward an unwarranted invasion of privacy, he said. Justice Stevens concluded

The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of "what the Government is up to," the privacy protected by Exemption 7(C) is in fact at its apex while the FOIA-based public interest in disclosure is at its nadir. Such a disparity on the scales of justice holds for a class of cases without regard to individual circumstances; the standard virtues of bright-line rules are thus present, and the difficulties attendant to ad hoc adjudication may be avoided. Accordingly, we hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no "official information" about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is "unwarranted."¹¹¹

Scores of federal agencies routinely compile information pursuant to the statutory duties that, of itself, is not "official information about a Government agency." Based on the reasoning of Reporters Committee, it remains to be seen what other categorical exemptions to the FOIA executive agencies might attempt to carve out. And once agencies attempt to routinely exclude classes of information, the courts, which are the designated arbiters

of FOIA disputes, must defer to the agency's judgment unless the requester can show the information relates specifically to the agency's conduct. This imposes a difficult burden on the requester, especially when amorphous compilations of information are involved. In such cases, the relevance of information to agency conduct might be shown only after receipt and analysis of the challenged information.¹¹²

Cases Decided Since Reporters Committee

Since Reporters Committee, several courts have relied on the case in opinions limiting access to government-held information on privacy-related grounds. In National Association of Retired Federal Employees v. Horner, the U.S. Court of Appeals for the District of Columbia Circuit interpreted Reporters Committee as limiting a court's public interest inquiry to the nature of requested information and its relationship to the FOIA without looking at other potential societal benefits.¹¹³ The case involved a request by the NARFE for the computerized names and addresses of persons added to federal annuity rolls, held in a government data base. The lower court had allowed disclosure, reasoning that the relatively minor privacy infringement by disclosure of only names and addresses was outweighed by "the public interest in disclosure that flows from the NARFE's service and the fact that many annuitants might be pleased to learn of them."¹¹⁴ The D.C. Circuit rejected this balancing approach that looked at the result of disclosure,

noting instead that "the [FOIA's] sole concern is with what must be made public and not made public."¹¹⁵ Finding no public interest in such disclosure under the Reporters Committee reasoning, the court held that even the minor privacy infringement of disclosing names and addresses tipped the balancing scales in favor of withholding the information.

The reasoning of Reporters Committee was central to the D.C. Circuit's reasoning in American Federation of Government Employees v. Department of Health and Human Services, a case involving the privacy interests of people whose names and addresses were contained in an agency's data base. The D.C. Circuit held that the public interest embodied in a collective bargaining statute, which had no direct bearing on an agency's performance, was insufficient to overcome the minor privacy interests of the information.¹¹⁶

Reporters Committee also was relied on by a federal district court in New York in a case challenging portions of the state's Ethics in Government Act. In Igneri v. Moore, the court concluded that a requirement that county committee chairpersons file annual disclosure statements with the Ethics Commission violated their right of privacy.¹¹⁷ The court cited Reporters Committee's reasoning that privacy interests in avoiding further disclosure remain intact, notwithstanding the presence of the information in public

records. The court also followed the Reporters Committee definition of informational privacy as, among other things, the right of individuals to control information about themselves.¹¹⁸

A New Jersey superior court cited Reporters Committee's reasoning that information in government compilations posed a greater privacy threat than the information at its original source. In Asbury Park Press, Inc. v. Department of Health, the court affirmed a lower court's denial of a newspaper request for hospital data compiled by the New Jersey Department of Health.¹¹⁹ The court, suggesting a categorical approach to shielding computer compilations, held that when balancing the public interest in disclosure with privacy concerns, the balance tips in favor of privacy when public information is a compilation rather than its original form.¹²⁰

Privacy-Access Cases Addressing Technical and Definitional Concerns

While much of the foregoing analysis has focused on the constitutional question of informational privacy and on the Supreme Court's interpretation of privacy in the public policy arena, privacy concerns have affected access to computerized government information at a more practical level. As outlined previously, technical and definitional problems related to privacy concerns also threaten to limit access to computerized records. Technical problems arise when agency personnel simply are unwilling or unable to use

computers to provide meaningful access. Definitional problems occur because records laws, written when most records were in paper form, do not resolve novel issues posed by computerized records. This section looks at how federal and state courts have attempted to deal with such technical and definitional problems of computer access. Some of the court cases that follow do not dispute the private nature of personal information; rather, they deal with issues, such as agencies' duty to segregate exempt and non-exempt information in a computer, that have a direct bearing on access when privacy is a concern. Some opinions also broach the broader public policy issues related to computer access. The various cases often deal with several related issues, some of which overlap.

Federal Courts and Technical and Definitional Privacy Concerns

Several federal court cases offer insight into the technical and definitional problems related to privacy that arise when government records are computerized. As discussed in Chapter Two, federal courts have said that information in agency computers is as much a public record as paper records would be.¹²¹ But even working from this assumption, courts have had difficulty applying paper-era statutes to computer record issues with consistent results.

Duty to Create a Record

It is well established that federal agencies do not have to create records to comply with FOIA requests.¹²² In

the case of paper records, the duty was clearly defined: Agencies are not required to gather information from various sources to create new documents or to analyze or summarize information in their files; such a duty would impose too great a burden on agency personnel. However, what constitutes "creation" of a record when the time-saving capabilities of computers are factored in is much less clear.

For example, in the 1982 case Yeager v. DEA, a requester sought information contained in an agency computer that, as it existed, was shielded from disclosure under an exemption to the Freedom of Information Act.¹²³ The request comprised four complete data systems, with personal identifying information deleted, along with supporting computer software. The requester argued in court that the FOIA imposed a duty on the agency to use "disclosure-avoidance techniques" to render information disclosable.¹²⁴ In effect, the requester was asking the agency to use its computers to edit the information to shield exempt, personal material so the request could be met without triggering the FOIA exemption. The U.S. Court of Appeals for the District of Columbia Circuit rejected this reasoning. The court concluded agencies were not required under the FOIA to create a new record by using their computer capabilities to "compact" or "collapse" information to eliminate privacy concerns.¹²⁵

In Long v. IRS, the U.S. Court of Appeals for the Ninth Circuit reached a different conclusion in a similar situation.¹²⁶ The Internal Revenue Service argued that providing a computer tape with some private information deleted constituted creation of a new record, which the FOIA did not require. The court rejected the IRS's argument, holding that deletion of identifying information to ensure personal privacy was permissible and that the result was not a "new record" for FOIA purposes.¹²⁷

Creation of a Computer Program to Meet FOIA Requests

An issue related to the question of whether generating a document from a computer is "creating" a record is whether agencies must develop computer programs to compile or organize information to meet FOIA requests. A federal district court in Pennsylvania said creation of a special computer program to meet a public record request exceeded the Treasury Department's obligations to provide records under the FOIA. The case, Clarke v. U.S. Department of Treasury, arose when an individual asked the department for names and addresses of all registered institutional owners of certain kinds of bonds, along with dollar amounts, maturity dates, and ownership of each bond.¹²⁸ The Treasury Department refused the request because such information did not already exist as an agency record. The requester argued that the information was neither privileged nor confidential and that a computer program could be written to extract the

requested information. However, the court said that "while an agency may be required to produce records that do exist, it is not required to make them."¹²⁹ The court also noted that the Treasury Department's own regulations provide that "[t]here is no requirement that records be created or data processed in a format other than required for government purposes" to comply with a request.¹³⁰

Segregation of Computerized Data

Another situation that has posed difficulties for computerized access--and the one most directly related to privacy concerns--arises when information disclosable under the FOIA is intermixed in government computers with exempt information. In such instances, the FOIA requires agencies to provide "[a] reasonably segregable portion of a record . . . after deletion of portions which are exempt."¹³¹ The understanding of what steps agencies should reasonably take to provide access evolved when deletion of exempt material consisted of manually blacking out the information in each document. Based on several cases, federal courts have established several criteria for determining whether nonexempt material is reasonably segregable from exempt material. First, agencies need not segregate information--and may deny access--when the result of the editing would be an unintelligible document.¹³² Second, agencies can refuse to segregate when disclosable material is so inextricably intertwined with nondisclosable information that segregation

is not feasible and would place an inordinate burden on an agency.¹³³ Third, disclosure would not be required when disclosable material is largely interspersed with nondisclosable information, once again resulting in a document that does not meaningfully represent the record as a whole.¹³⁴ Finally, agencies may withhold nonexempt information that would be revealing and endanger the confidentiality of exempt information in it.¹³⁵

When records are stored in computers, the issue of the ability to segregate becomes more complex. In some cases, deletion of exempt material requires record custodians to go through complex steps or to create special computer programs. But, in many instances, deletion of exempt information can be accomplished with several keystrokes. Still, agencies sometimes have been reluctant to recognize that properly designed computers make it easier for them to segregate information, and they balk at the idea of deleting exempt material to facilitate disclosure.

Two circuits of the U.S. Court of Appeals have attempted to deal with the question of segregating information in government computers. Each court reached a different result. In 1980, the Ninth Circuit said that "editing" identifying information on individual taxpayers to satisfy an FOIA request was within the scope of an agency's duty to segregate exempt and nonexempt information. In Long v. IRS, the court said it did not believe the "mere deletion

of names, addresses, and social security numbers to protect privacy resulted in the agency's creating a whole new record."¹³⁶ However, the court was not clear about the agency's duty to create a computer program to edit out such information.

Two years later, in Yeager v. DEA, the D. C. Circuit reached a different conclusion when it considered "the extent to which an agency is required to employ its computer capabilities in fulfilling its duty to segregate and release nonexempt material."¹³⁷ The case began with a request for several entire DEA computer files on narcotics violations--information normally shielded by an FOIA exemption. The requester asked that the DEA "collapse" the records, a relatively complex process using the computer to eliminate personal, identifying information and leaving only disclosable aggregate data. The court refused to require the agency to collapse information, maintaining that the FOIA "does not contemplate imposing a greater segregation duty upon agencies that choose to store records in computers than upon agencies that employ manual retrieval systems."¹³⁸ In other words, the court said that even though an agency's computers can perform certain tasks that make data lawfully disclosable, the agency's only duty is to perform tasks analogous to segregating information in paper format. The Yeager court concluded that "the FOIA does not mandate that the DEA use its computer capabilities to 'compact' or

'collapse' information as part of its duty to disclose reasonably segregable information."¹³⁹ However, the court did suggest that computers provide agencies with more flexibility to meet FOIA requests and said that agencies should be encouraged to "perform services agencies are not required to provide."¹⁴⁰

Duty to Invest in New Computer Technology

A question somewhat related to the duty of agencies to segregate exempt and nonexempt information is whether agencies must invest in new computer technology to aid public access. While the Yeager court encouraged agencies to use computers voluntarily to go beyond the letter of access law to meet FOIA requests, the extent to which agencies are obligated to invest in new computer capabilities to enhance access is limited. In 1986, a federal court in Florida said the U.S. Customs Service was not obliged to invest in costly technology to provide public access terminals. In Martin & Merrell, Inc. v. United States Customs Service, an FOIA requester seeking certain liquidation entries on file with the Customs Service asked the service's Miami division to install on-site computer terminals so information could be accessed without filing a FOIA request.¹⁴¹ The court said, "The [FOIA] in no way contemplates that agencies . . . should invest in the most sophisticated and expensive form of technology."¹⁴²

State Courts and Computer Access Issues

While federal courts have been active in attempting to deal with a range of technical and definitional issues related to computers and personal privacy, state courts have tackled many of the same problems. Some courts have supported withholding of personal information simply because it was in a computer, even when the information was not highly personal. Other state courts have looked beyond the physical form of the information, focusing instead on its content.

The Colorado Supreme Court embraced the notion that computerized information was inherently threatening to privacy. In 1972, as congressional hearings leading to passage of the federal Privacy Act were hitting full stride, the Colorado court decided a case that concluded the very nature of computerized personal information posed a threat to privacy. In Davidson v. Dill, a woman acquitted of a municipal loitering charge sought to have her arrest record expunged or returned to her.¹⁴³ She had been photographed, fingerprinted, and required to furnish personal information about herself, which remained in police files after her acquittal. A trial court rejected her request, which was based on a claim that the police had no statutory authority to retain such records, and that to do so would constitute an invasion of her privacy.¹⁴⁴ The Colorado Supreme Court reversed the lower court and remanded the case, suggesting

the threat to her personal privacy was exacerbated by "modern technology." The court, citing Arthur Miller's influential book The Assault on Privacy,¹⁴⁵ said,

Recent years have witnessed a substantial upsurge in the number of cases and commentaries dealing with the problem before this Court. In no small part, this phenomena is due to the advent of the computer age--an event which has drastically increased the power of industry and government to collect data--and the growing concern for the individual's loss of privacy as a natural by-product of our modern technology.¹⁴⁶

The court noted that such arrest files, which often did not reflect whether charges were later dropped or suspects exonerated, were routinely shared with other law enforcement agencies. These agencies included the Federal Bureau of Investigation, which maintained computer data bases of such records. The court concluded that maintaining such files, unless the police could establish a compelling need to retain the information, conflicted with an emerging right of privacy.¹⁴⁷ The court said,

Notwithstanding the absence of a conviction, the mere record of arrest often works as a serious impediment and basis of discrimination in the search for employment, in securing professional, occupational, or other licenses, and in subsequent relations with the police and the courts.¹⁴⁸

In 1982, the Michigan Supreme Court rejected a request for names and addresses that were to be published in a student directory because the list was computerized and posed a threat to the students' privacy. The case, Kestenbaum v. Michigan State University, began when a student filed a lawsuit seeking a computer tape containing

the names and addresses of students attending Michigan State University.¹⁴⁹ The university used the tape to produce the university's directory of names and addresses, which was publicly distributed. The court rejected the request on the basis of the students' rights of privacy, even though the student information would eventually be disseminated publicly in the student directory. Focusing on the computerized form of the information, the court said, "Form, not just content, affects the nature of information. . . . Seemingly benign data in an intrusive form takes on quite different characteristics than if it were merely printed."¹⁵⁰ The court further reasoned that students were not aware when they registered at the university that "an efficient and intrusive computer mailing system already was available to anyone at a nominal sum."¹⁵¹

Two years later, in 1984, the Michigan Supreme Court followed Kestenbaum when it held that the Detroit Police Department was correct in denying a request for a computer tape that contained traffic accident information available in paper format from public records. In Mullin v. Detroit Police, the plaintiff sought a computer tape containing the names and addresses of people involved in traffic accidents in Detroit during a certain period.¹⁵² The same information was contained in some 70,000 accident reports, which were public records. The court concluded the case fell squarely within Kestenbaum, which recognized special privacy dangers

inherent in computerized information. In fact, the court reasoned that greater privacy interests were at stake in the Mullin case because the accident reports contained not only names and addresses but also embarrassing facts, such as the names of people who had been arrested. On this basis, the court held that disclosure of the computer tape based on public records would constitute a "clearly unwarranted invasion of privacy."¹⁵³

In 1988, a Massachusetts appeals court blocked release of driver's license records out of concern for the "aggregate effect" of such disclosure on privacy. In Doe v. Registrar of Motor Vehicles, the court vacated a lower court decision allowing disclosure of driver's records.¹⁵⁴ The court placed the burden on the record custodian to show that information was not "personal data" under the state's Fair Information Practices Act before disclosing it. Then, in reasoning that focused on the quantity of information stored in an agency's computer rather than on the harmful effect disclosure might have on individual privacy, the court said,

Even if the items here at issue are not considered "intimate details of highly personal nature," the aggregate effect on the privacy of the total number of people whose data are documented weighs against disclosure. . . . There is a negative public interest in placing the private affairs of so many individuals in computer banks available for public scrutiny.¹⁵⁵

The preceding state cases show some courts have concluded that computers pose a special threat to privacy, even when computerized information was not highly personal

in nature and when the information was available elsewhere in public records. Other courts, however, have treated computerized records just as they would paper records and have allowed the same level of access.

For example, in the 1976 case Beacon Journal Publishing Co. v. Andrews, the Supreme Court of Ohio held that the Registrar of Motor Vehicles had to make edited printouts of motor vehicle violations available to a newspaper at cost within a reasonable amount of time, even though the registrar maintained private information on driver's license applications in the same computer data base.¹⁵⁶ The Beacon Journal had sought a printout of motorists who had exceeded bad-driving point limits, along with any records of steps taken by the state to suspend the licenses of those motorists. The registrar balked, contending that such printouts would contain private driver's license information, that the costs and time necessary to set up the computer to analyze the printouts for accuracy would be prohibitive, that filling such a large request would take excessive time and take employees away from their normal duties, and that such disclosure would violate the right of privacy of citizens.¹⁵⁷ The court was unsympathetic, reasoning that the registrar was under a statutory duty to organize his office and employ his staff in such a way that record access requests could be met in a timely and cost effective manner.¹⁵⁸

A Louisiana appeals court reached a similar result in Webb v. Shreveport,¹⁵⁹ in which the court upheld a request for a computer tape containing the names and addresses of public employees in Shreveport. The court said that because the names and addresses were in public records in other forms, no reasonable expectation of privacy existed for the same records in computer format under privacy provisions of the state's constitution.¹⁶⁰ While the court held there was no privacy expectation in the public-record information in question, it did not specifically discuss whether computerized records pose a privacy threat greater than paper records.¹⁶¹

Computer records received a similar assessment, by a New York court, in Szikszay v. Buelow.¹⁶² In Szikszay, the plaintiff sought computer tapes containing names and addresses of all of a county's property owners. The court held that the computer tapes were public records and must be disclosed under the New York Freedom of Information Law. The court explicitly rejected any distinction between computerized public records and their paper counterparts and found no unwarranted invasion of privacy. "The form of the records and the petitioner's purpose in seeking them do not alter their public character or petitioner's concomitant right to inspect and copy," the court said.¹⁶³

In 1982, the Kansas Supreme Court also treated computerized records the same as those in any other form.

In Stephan v. Harder, a case that has been widely cited, the court held that computer tapes containing the names and addresses of physicians who received public funds for performing abortions were public records.¹⁶⁴ The court reasoned that because the computer tapes were required to be maintained by Kansas law, they were public records. The court also held that editing the computer tapes to remove private information did not constitute creation of "new records" because custodians had a duty to segregate exempt and nonexempt information to meet public record requests. In addition, the court reasoned that any privacy interests the physicians might have were outweighed by the public's right to know about the workings of government.¹⁶⁵

In 1984, the Connecticut Supreme Court also addressed how far agencies must go to segregate exempt and nonexempt information, in holding that a state welfare agency could be compelled to provide to a newspaper information from computerized welfare records.¹⁶⁶ In Maher v. Freedom of Information Commission, the court said the public interest in disclosure set forth in the state Freedom of Information Act must be weighed against the potential danger to the privacy interests of individual welfare recipients. To overcome privacy concerns and tip the balance in favor of the public interest in disclosure, the court said the Freedom of Information Commission must first obtain assurances of "the virtual impossibility of identifying

individual Medicaid recipients from the records whose release has been ordered."¹⁶⁷

In Family Life League v. Department of Public Aid, the Illinois Supreme Court said the fact records kept by welfare abortion providers pursuant to state record laws contained names of abortion recipients did not prevent disclosure of nonprivate information.¹⁶⁸ The case arose when an anti-abortion organization sued the state Department of Public Aid seeking records about public funds paid to doctors and medical providers for welfare abortions and abortion-related services. A lower court ordered the state to provide the addresses of doctors and providers of abortion services, and the state appealed. On appeal, the state presented four arguments against disclosure: It would violate the patients' right of privacy; it would have an inhibiting effect on abortion providers, thus indirectly affecting abortion patients' right of privacy; it would invade the privacy of abortion providers; and compliance would require creation of a "new record," which was not required of agencies.¹⁶⁹ The high court rejected the arguments, holding the state's public records law required disclosure of the information, with the names of abortion recipients deleted, in a reasonable amount of time. However, the court said the requester of the records must pay the cost of a computer program necessary to segregate the information to meet the request.¹⁷⁰

Several state courts have agreed that school districts could release nonidentifying aggregate information about students without endangering their privacy. The cases involved attempts by individuals and organizations to obtain access to information related to overall student performance. At issue was whether school districts had a duty to remove identifying personal information to make meaningful statistical data available to the public.

In 1980, in Kryston v. Board of Education, East Ramapo Central School District, a New York appellate court held that disclosure of certain standardized reading and mathematics test scores, in "scrambled" order and with names deleted, would protect the privacy of students and impose no onerous burden on the school system.¹⁷¹ The case began when the parent of a student in the school district sought reading and math scores on certain standardized tests given to third-grade students during a school year. The school district refused to provide the scores, which were compiled in alphabetical order, and was upheld by a lower court, which cited student privacy provisions of the Family Educational Rights and Privacy Act.¹⁷² The court reasoned that release of the alphabetized scores, even with the names deleted, could lead to identification of individual students because the list consisted of only 75 scores. The court acknowledged that the identification problem could be resolved by scrambling the scores but held the school

district had no duty to prepare a new record to make information disclosable.¹⁷³ The appellate court, construing the state's public records law to be applied liberally "to permit maximum access to documents," held that the school district must scramble the records and make them available. "Disclosure of the test scores here, in a 'scrambled' order and with names deleted, would protect the privacy of the students, provide the petitioner with the records she seeks, and impose no onerous burden upon the agency."¹⁷⁴

In 1986, a Colorado appeals court reached the same conclusion in Western Services, Inc. v. Sargent School District No. RE-33J.¹⁷⁵ A nonprofit corporation working to improve the quality of education in schools attended by Hispanic children sought scores on basic skills tests by grade level and coded to identify the ethnic background of the test-taker. A trial court granted the school district a summary judgment, denying access to the records because they were "scholastic achievement data on individual persons" and, therefore, exempt under the state open records law.¹⁷⁶ The appellate court reversed the lower court and remanded the case. The appellate court rejected the school district's argument that because exempt and nonexempt information were mixed, the district would have to create a new record to comply with the data request. The appellate court concluded,

We hold that under our public records act there exists an implied duty to delete exempt

information from that which may be disclosed, and to structure the record to provide the information which the public is entitled to have. Here, that duty includes scrambling the order of the test-takers contained in the class record sheet and coding Hispanic surnamed individuals to show their ethnic origin.¹⁷⁷

The appellate court also put to rest an assertion by the school district that the state law applied only to "records" and not to "information." Said the court, "For the purposes of this case this is a distinction without a difference. Information does not exist in a vacuum. Rather, a 'record' by its very nature exists to impart the information contained in it."¹⁷⁸

In another 1986 case, the Illinois Supreme Court held that a school district must disclose masked and scrambled records of achievement test scores. In Bowie v. Evanston Community Consolidated School District No. 65, parents sought disclosure of standardized test scores for students for certain years, grades, and schools in the district, along with a list of educational programs available in those schools.¹⁷⁹ The parents filed suit after the district denied their request, and a circuit court dismissed the parents' complaint on two grounds. First, the court cited the privacy rights of the students; second, the court concluded a school "status report" issued by the district provided sufficient information to satisfy the parents' request. The parents appealed. On appeal, the district argued that the information was private and, therefore, exempt and that to

mask and scramble the information would be "unduly burdensome."¹⁸⁰ The appellate court disagreed. It held that an agency that maintained record systems containing both exempt and nonexempt records had a duty to separate the records to meet access requests and that to do so did not constitute creation of a new record. The court also was satisfied that masking and scrambling the records were sufficient to protect the privacy of the students.¹⁸¹

Privacy/Access Out of Balance

The computer has altered the privacy-access equation in ways not foreseen when laws such as the federal Freedom of Information Act first aimed at delineating how and under what conditions members of the public would have access to information--about themselves and about the government serving them. Mechanical and definitional incongruencies alone, between paper and computerized records, have been sufficient at times to derail access to information. Consequently, when courts have decided disputes over information held in government computers, outcomes generally have been unpredictable. Court opinions vary, for example, on the stature of records once they are computerized--on whether they must be viewed tantamount to paper records.

Yet, it is the question of public policy that seems to overshadow technical and definitional concerns--niggling problems that, however threatening to access they at times may be, can be grasped and addressed and, it is hoped,

resolved in some manner. Public policy, based in general on a nation's attitude, presents an entirely different kind of problem. Nowhere in the privacy-access debate has this been more apparent than in the decision of the Supreme Court in Reporters Committee. The nation's highest court explicitly recognized a right of informational privacy seemingly on a par with other constitutional privacy interests acknowledged by the Court. At the core of the majority opinion in Reporters is a public policy question about the very nature of computers and their potential impact on America--a question that shifts the focus away from the content of information to its form. A native fear of technology and the danger it poses for individual freedoms resonates in the opinion written by Justice John Paul Stevens, who framed the issue as "whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by the disclosure of that information."¹⁸²

Notes

1. United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989); (hereafter referred to as Reporters Committee). See also U.S. Department of Justice Office of Policy Development, FOIA Update 3 (Spring 1989) for the Justice Department's interpretation of Reporters Committee. Based on this interpretation, the Justice Department provides legal advice to federal executive agencies.

2. See William Prosser, "Privacy," 48 Calif. L. Rev. 383 (1960).

3. See generally the Privacy Act, 5 U.S.C. sec. 552a (1974), and related legislation, discussed in Chapter Three.

4. Stanley v. Georgia, 394 U.S. 557 (1969).

5. Katz v. United States, 389 U.S. 347 (1967).
6. NAACP v. Alabama, 357 U.S. 449 (1958).
7. Griswold v. Connecticut, 381 U.S. 479 (1965).
8. Roe v. Wade, 410 U.S. 113 (1973). See also Planned Parenthood of Southeastern Pennsylvania v. Casey, U.S. _____ (1992), 60 U.S.L.W. 4795, 1992 WL 142546, upholding a constitutional right to an abortion.
9. Whalen v. Roe, 429 U.S. 589 (1977).
10. Reporters Committee, *supra* note 1.
11. Pope v. Curl, 2 Atk. 324, 26 Eng.Rep. 608 (1741).
12. David H. Flaherty, Privacy in Colonial New England 121 (1972).
13. Restatement (Second) of Torts sec. 652D (1977).
14. See generally Ethan M. Katsh, The Electronic Media and the Transformation of Law (1989); and Ithiel De Sola Pool, Technologies of Freedom (1983).
15. Paul v. Davis, 424 U.S. 693 (1976).
16. Id. at 713.
17. United States v. Miller, 425 U.S. 345 (1976).
18. Katz v. United States, 389 U.S. 347, 353 (1967).
19. United States v. Miller at 442-443.
20. Reported in Flaherty, Privacy in Colonial New England at 5. See also Charles Fried, An Anatomy of Values 140-141 (1970). Fried, viewing privacy as a fundamental value, said,

Privacy, thus, is control over knowledge about oneself. But it is not simply control over the quantity of information . . . there are modulations in the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details. For instance, a casual acquaintance may comfortably know that I am sick, but it would violate my privacy if he knew the nature of the illness. Or a friend may know what particular illness I am suffering from, but

it would violate my privacy if he were actually to witness my suffering from some symptoms which he must know is associated with the disease. . . . Privacy in its dimension of control over information is an aspect of personal liberty. Acts derive their meaning partly from their social context--from how many people know about them and what the knowledge consists of.

21. United States v. Miller at 449, quoting Burrows v. Superior Court, 529 P.2d 590 (1974).

22. Privacy Act of 1974, 5 U.S.C. sec. 552a et seq.

23. 12 U.S.C. sec. 3401.

24. Whalen v. Roe, supra note 9.

25. Pub. Health Law N.Y. sec. 3300 et seq. McKinney, Supp. 1976-1977.

26. Whalen v. Roe, 403 F.Supp. 931 (S.D.N.Y 1975).

27. Whalen v. Roe at 598.

28. Id. at 591.

29. Id. at 598.

30. Id.

31. Id. Justice Stevens cited an independent investigation into computerized central filing systems in California and Illinois. The investigation failed to uncover a single case in which a patient's privacy was violated.

32. Id. at 600.

33. Id. at 605.

34. Id. at 605-606. Justices Stevens cited Arthur Miller, "Computers, Data Banks and Individual Privacy: An Overview," 4 Colum. Hum. Rts. L. Rev. 1 (1972), and Arthur Miller, The Assault on Privacy: Computers, Data Banks and Dossiers (1971). Both the law review article and book by legal scholar Miller, as well as his testimony before several congressional committees, were instrumental in passage of the Privacy Act of 1974.

35. Id. at 606.

36. Id. at 606-607.
37. Reporters Committee, supra note 1.
38. Id.
39. Computer Security Act of 1987, Pub. L. No. 100-235.
40. Interestingly, the Privacy Act allows agencies to collect only information necessary to perform their statutory duties. Under this reasoning, all agency information is, at least indirectly, relevant to agency performance.
41. Reporters Committee at 757.
42. Id.
43. Id.
44. Id.
45. Id.
46. Id., citing 28 U.S.C. sec. 534.
47. Freedom of Information Act, 5 U.S.C. secs. 552b(3) (A) and 552b(3) (B).
48. Reporters Committee at 757. See 5 U.S.C. 552b(6). Exemption 6 shields information in personnel, medical, and "similar" files, the disclosure of which "would constitute a clearly unwarranted invasion of personal privacy."
49. Id.
50. Id.
51. Id., quoting the district court's summary judgment opinion.
52. Id. at 759.
53. Id., citing Reporters Committee for Freedom of the Press v. United States Department of Justice, 816 F.2d 730 (D.C. Cir. 1987).
54. Id. at 759.
55. Id.

56. Id.
57. Id., citing Reporters Committee for Freedom of the Press v. Justice Department, 831 F.2d 1124 (D.C. Cir. 1987).
58. Id.
59. Id. at 1124, 1126.
60. Id.
61. Id.
62. Petitioners' brief for certiorari, at 11-12. United States Department of Justice v. Reporters Committee for Freedom of the Press, 485 U.S. 1005 (1988), cert. granted.
63. Department of Justice v. Reporters Committee for Freedom of the Press, 485 U.S. 1005 (1988).
64. Reporters Committee, supra note 1.
65. Id. at 780-781. Justice Blackmun, in his concurring opinion joined by Justice Brennan, generally supported the majority result. However, he took issue with the majority's position on categorical balancing. He said,
- Such a bright-line rule obviously has its appeal, but I wonder whether it would not run aground on occasion, such as in a situation where a rap sheet discloses a congressional candidate's conviction of tax fraud five years before. Surely, the FBI's disclosure of that information could not "reasonably be expected" to constitute an invasion of personal privacy, much less an unwarranted invasion.
66. Id. at 762.
67. Id., citing Whalen v. Roe at 598-600.
68. Id.
69. Individuals do have some control over information about themselves in the criminal justice context, but it requires assistance from a court. For example, an individual can petition a court to have a criminal record sealed or expunged.
70. Reporters Committee at 763-764, quoting Webster's Third New International Dictionary of the English Language,

Unabridged 1804 (1976). The dictionary defines information as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public."

71. Id.

72. Id., citing Samuel Warren and Louis Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193, 198 (1890).

73. Id. at 764-765.

74. Id. at 753.

75. Id. at 752, citing 28 U.S.C. sec. 534(b). Interestingly, the concern about widespread dissemination expressed in 28 U.S.C. sec. 534(b) was not about public record information contained in criminal history files, but rather for uncorroborated or hearsay information and outdated information, such as charges that were filed but later dropped. Also, the legislative history of the original FOIA Exemption 7(C) focused on the potential harm disclosure would pose to investigations, not to individuals.

76. Id. at 765, citing the Privacy Act of 1974, 5 U.S.C. sec. 552a. and quoting H.Rep. No. 93-1416, 7 (1974).

77. Congress, reacting to several conflicting court opinions that attempted to use the Privacy Act as justification for withholding information, amended the Privacy Act in 1974 to specifically state that the act was not an Exemption 3 statute under the Freedom of Information Act. The new language was achieved as an amendment to the National Security Act of 1947 (50 U.S.C. sec. 431). See Thomas M. Susman, "The Privacy Act and the Freedom of Information Act: Conflict and Resolution," 21 J. Marshall L. Rev. 703 (1988).

78. Reporters Committee at 766.

79. Id. at 765.

80. Id.

81. Id. The FOIA language, however, also was an acknowledgement by Congress that all information held by agencies was disclosable, unless covered by a specific FOIA exemption, of which the Privacy Act was not. See supra note 77.

82. Id. at 767.

83. Department of Air Force v. Rose. 425 U.S. 352 (1976).
84. Reporters Committee at 768.
85. Id. at 769.
86. Id. at 770, citing Whalen v. Roe at 605.
87. Id. at 770-771, citing William Rehnquist, "Is An Expanding Right of Privacy Consistent with Fair and Effective Law Enforcement," 1 Nelson Timothy Stephens Lectures 13, University of Kansas Law School (September 26-27, 1974).
88. Reporters Committee at 773.
89. Id.
90. Id. at 771.
91. Id., citing Department of Air Force v. Rose at 372.
92. Id. at 775.
93. Reporters Committee at 775.
94. Id. at 772-773.
95. Brown v. FBI, 658 F.2d 71, 75 (2d Cir. 1981).
96. Lloyd & Henninger v. Marshall, 526 F.Supp. 485, 487 (M.D. Fla. 1981).
97. Multnomah County Medical Society v. Scott, 825 F.2d 1410 (9th Cir. 1987).
98. Minnis v. Department of Agriculture, 737 F.2d 784 (9th Cir. 1984) cert. denied 471 U.S. 1053 (1985).
99. Wine Hobby USA, Inc. v. IRS, 502 F.2d 133 (3d Cir. 1983).
100. Columbia Packing Co. v. Department of Agriculture, 563 F.2d 495 (1st Cir. 1977).
101. Id. at 499-500.
102. Cochran v. United States, 770 F.2d 949 (11th Cir. 1985).

103. Id. at 956.

104. Id. at 958.

105. International Board of Electrical Workers v. Department of Housing and Urban Development, 852 F.2d 87, 90 (3d Cir. 1988).

106. NLRB v. Sears, Roebuck & Co., 421 U.S. 132 (1975).

107. Id. at 174, citing S. Conf. Rep. No. 93-1200 (1974), in U.S. Code Cong. & Admin. News 6267 (1974).

108. See supra note 62.

109. Reporters Committee at 776.

110. Id.

111. Id. at 780.

112. Chapter One cites examples of how independent analysis of agency information can lead to conclusions not readily apparent or not contained in any "traditional" document. For example, a newspaper's analysis of an Internal Revenue Service computer data base disproved an IRS claim that underpayment of taxes had risen sharply during the previous 20 years. See Katherine Corcoran, "Power Journalism," News Inc., November 1991, at 30. See also Mitchell Hartman, "Investigative reporters use databases to break stories," The Quill, November/December 1990, at 21-26.

113. National Ass'n of Retired Federal Employees v. Horner, 879 F.2d 873 (D.C. Cir. 1989).

114. Id. at 874-875.

115. Id., citing Reporters Committee at 771.

116. American Federation of Government Employees v. Department of Health and Human Services, No. 89-444 (1989). See Access Reports, Nov. 29, 1989, at 9.

117. Igneri v. Moore, 721 F.Supp. 406 (N.D.N.Y. 1989).

118. Id. at 411.

119. Asbury Park Press, Inc. v. Department of Health, 558 A.2d 1363 (N.J. 1989).

120. Id. at 1366-1367.

121. See e.g., Yeager v. DEA, 678 F.2d 315 (D.C. Cir. 1982). The Yeager court made clear that computer-stored records, whether stored in a central processing unit, on magnetic tape, or in some other form, were records for purposes of the Freedom of Information Act.

122. See generally Forsham, National Relations Board v. Sears & Roebuck Co., 421 U.S. 132, 162 (1975); Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136, 153 (1980).

123. Yeager v. DEA, supra note 121.

124. Id. at 317.

125. Id. at 327.

126. Long v. IRS, 596 F.2d 362 (9th Cir. 1979) cert. denied 466 U.S. 917 (1980).

127. Id. at 366.

128. Clarke v. U.S. Department of Treasury, Civ. A. No. 84-1873 (E.D. Pa. 1986). Unreported. 1986 WL 1234 (E.D. Pa. 1986).

129. 1986 WL 1234 at 1, citing Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136, 152 (1980).

130. Id. at 2-3.

131. 5 U.S.C. sec. 552(b).

132. See Lead Industry Ass'n v. OSHA, 610 F.2d 70, 85-87 (2nd Cir. 1979).

133. See Mead Data Cent., Inc. v. Department of Air Force, 566 F.2d 242, 260 (D.C. Cir. 1977).

134. See Lead Industry Ass'n v. OSHA, supra note 132; Sterline Drug, Inc. v. Harris, 488 F.Supp 1019 (S.D.N.Y. 1980).

135. See Lead Industry Ass'n v. OSHA, supra note 132, at 86.

136. Long v. IRS at 366.

137. Yeager v. DEA, supra note 121.

138. Id. at 322.

139. Id. at 327.
140. Id. at 326.
141. Martin & Merrell, Inc. v. United States Customs Service, 657 F.Supp. 733 (S.D. Fla. Nov. 1986).
142. Id. at 734.
143. Davidson v. Dill, 503 P.2d 157 (1972).
144. Id. at 158.
145. Miller, The Assault on Privacy, supra note 34.
146. Davidson v. Dill. at 158.
147. Id. at 160.
148. Id. at 159.
149. Kestenbaum v. Michigan State University, 327 N.W.2d 783 (1982).
150. Id. at 789.
151. Id. at 790.
152. Mullin v. Detroit Police, 348 N.W.2d 708 (1984).
153. Id. at 712.
154. Doe v. Registrar of Motor Vehicles, 528 N.E.2d 880 (1988).
155. Id. at 886.
156. Beacon Journal Publishing Co. v. Andrews, 358 N.E.2d 565 (Dec. 1976).
157. Id. at 566-577.
158. Id. at 569.
159. Webb v. Shreveport, 371 S.2d 316 (1979).
160. Id. at 317-318.
161. Szikszy v. Buelow, 436 N.Y.S.2d 558 (N.Y., Jan. 20, 1981).
162. Id. at 563.

163. Id.
164. Stephan v. Harder, 641 P.2d 366 (Kan. Feb. 17, 1982).
165. Id. at 374, 378.
166. Maher v. Freedom of Information Commission, 472 A.2d 321 (Conn. Feb. 21, 1984).
167. Id. at 327.
168. Family Life League v. Department of Public Aid, 493 N.E.2d 1054 (May 21, 1986).
169. Id. at 1056.
170. Id. at 1059.
171. Kryston v. Board of Education, East Ramapo Central School District, 430 N.Y.S.2d 688 (Aug. 11, 1980).
172. Id. at 689, citing 20 U.S.C. sec. 1232(g).
173. Id.
174. Id. at 690.
175. Western Services, Inc. v. Sargent School District No. RE-33J, 719 P.2d 355 (Jan. 1, 1986).
176. Id. at 356.
177. Id. at 357.
178. Id. at 357-358.
179. Bowie v. Evanston Community Consolidated School District No. 65, 538 N.E.2d 557 (April 20, 1989).
180. Id. at 559.
181. Id. at 560-561.
182. Reporters Committee at 764-765.

CHAPTER FIVE
TOWARD RESOLVING THE
COMPUTER PRIVACY/ACCESS ISSUE

Summarizing the Problem

Access to government information is recognized as an important social value, essential to democratic self-governance. The news media rely on government information for many of their news stories, which inform and educate the public about the workings of government and other issues that affect their daily lives and collectively influence the course of society.

More and more government information is being stored in computers, which is providing new opportunities for the news media to tell the public how government works--and sometimes fails to work. Journalists are just beginning to learn how to tap this new public resource as they go about fulfilling their historic roles as members of the Fourth Estate, the perennial watchdog of government. Examples of computer reporting successes abound, punctuated by the fact three recent Pulitzer Prizes for excellence in journalism were awarded for reports based on newspaper analysis of government data bases.¹

But the computerization of government information also increases the potential for invasion of personal privacy, another important social value. Access to government information has never been a given; at times it has required balancing the public interest served by disclosure with competing interests, such as privacy. Computers have thrown the traditional relationship between privacy and access, which developed over time, out of balance. This imbalance threatens to unnecessarily reduce access to government information and impede the flow of information about government to society.

If the individual is the heart of democracy, thinking and communicating free of interference, then an informed electorate is its head, making the decisions that, over time, affect generations to come. Individual privacy is highly valued, and rightly so, and it is understandable that it would be prized even more so today as an increasingly technological society threatens to erode it. But what is dangerous to a democracy is when one highly prized value--in this case privacy--is overprotected because of exaggerated or speculative fears that it might be lost, at the expense of another prized value, such as access to government information.²

An imbalance between access and privacy, caused by the computerization of government information, has occurred for several reasons. They include technical and definitional

issues, as well as more fundamental questions about the nature of computerized information and its potential to harm individuals.

Technical and definitional issues have threatened access even when the strength of the privacy interest favoring withholding of information was not in question. Rather, computerization has affected access because record keepers cannot--or will not--use the technology to ensure access to normally disclosable information.

Computerization also has affected access because it has confounded many of the laws and customs, developed when records were predominantly paper, that attempted to strike a balance between privacy and access. Definitions and interpretations that worked with paper documents often no longer effectively resolve access/privacy conflicts when information is contained in a computer.

The computerization of government also threatens access in a more fundamental way. Virtually from their introduction in government, computers often have been viewed as a potential threat to personal liberty, in particular the privacy of individuals about whom government keeps information. This long-standing concern about computers, while appropriate and well intentioned, nonetheless poses a threat to access when the form in which information is stored becomes more important than its content.

This concluding chapter will review the issues to show the importance of both privacy and access to government information in American society, to recount how the computer has confounded existing practice and policy regarding access to government information, and how fears about computers threaten to reduce such access. The chapter will state the belief that access and privacy can coexist, with protections for each, if policies developed when government information was kept on paper are revamped to account for today's technology. Therefore, it will advocate revision of the Freedom of Information Act, despite some inherent dangers in doing so, and will outline a descriptive model to illustrate how privacy and access can continue to be balanced in the computer age.

Access and Privacy: American Ideals

As preceding chapters have illustrated, privacy and access to government information both are values rooted deeply in the American experience.

During the Colonial period and the nation's formative years, privacy was evident as a social value; as a legal concept, it gained more recognition in the twentieth century as society grew complex and its technologies potentially more invasive.³ The modern computer, in particular, focused attention on privacy with its ability to store and process vast amounts of information. The debate in the 1960s over a proposal for a National Data Center--a central storinghouse

for information compiled by government to make sharing data easier--provided a forum for fears about advancing technology. Testimony was peppered with references to "Big Brother" of George's Orwell's novel 1984. Related hearings eventually led to legislative recognition of a right of privacy in the Privacy Act of 1974, followed by other computer-related legislation. In 1989, the Supreme Court underscored this concern about computers and privacy. In its Reporters Committee opinion, the Court arguably recognized a right of informational privacy, at times broaching constitutional analysis. The Court, echoing concerns raised by foes of the data center proposal three decades earlier, also concluded that compilations of personal information taken from generally accessible public records enjoyed a rejuvenated privacy interest when stored in government computers.⁴

While privacy evolved as a social and legal concept during the nation's development, the notion of a free and vigorous press as a watchdog on government also gained support from the Colonial period onward. To fulfill this role, the press must have access to government information, a fact recognized as a crucial tool in informing citizens about their government in a self-governing, democratic nation.⁵

As noted in Richmond Newspapers, the historial predicate of the public trial, a cornerstone of democracy,

was the English town meeting at which justice was meted out in public.⁶ The Constitution itself also supports the theory that the public's business should be public. By its own terms, the Constitution implies government secrecy is the exception, not the rule, and should be imposed only after a determination by Congress that secrecy served the common good.⁷

The need for access to government information also became a cornerstone of the twentieth-century theory of democratic self-government. Put forth eloquently by Alexander Meiklejohn, it said the fundamental role of the First Amendment was to ensure knowledgeable participation by citizens in a self-governed society.⁸

Legal scholar Vincent Blasi has amplified the need for an informed public in the democratic process, focusing on the role of the press as an essential check on the power of government. In his influential article titled "The Checking Value in First Amendment Theory," Blasi put great weight on the Founders' disdain for a government unbridled by a lack of public accountability. Writing soon after the much-publicized abuses by executive agencies during the Watergate scandal, Blasi envisioned the relation between the press and government as adversarial. But implicit in his checking value of the First Amendment was the need for access to the process and products of government. The press played such a crucial role, he reasoned, because government often

attempted to thwart legitimate access when it would result in exposure of mistakes and abuses.⁹

While the Supreme Court recognized a limited right of access to court proceedings in Richmond Newspapers and subsequent cases, it has stopped short of finding a right of access to government information generally. Chief Justice Burger, writing for the Court in the 1975 prison access case Houchins v. KOED, noted that the Court had "never intimated" a constitutional right of access to all government information (emphasis added).¹⁰ Instead, he concluded access to government information was a matter for the "political process."¹¹

Even though the Supreme Court has thus far refused to recognize a constitutional basis for a general right of access to government information, the "political process" has made clear such access is fundamental to democracy. Congress, whose members are the direct representatives of the people, has passed various measures acknowledging the public's right to know about the workings of government. Foremost among the legislation is the Freedom of Information Act, passed in 1966 after more than a decade of legislative hearings on issues related to public access. While the act itself contains no statement of purpose, its legislative history stated the act's aim was to foster "a general philosophy of full agency disclosure," subject only to specific, legislated exemptions.¹²

In sum, privacy and access to government information have been important values in American society. To coexist in a way that protects both, each must at times yield to the other in what legal scholar Alan Westin has called a "libertarian equilibrium."

When Values Collide

The courts have attempted to resolve privacy-related technical and definitional issues problems during the last two decades. The result, however, often was conflicting opinions, resulting in confusion for both the record custodians and those seeking access.¹³ Conflicting opinions between the District of Columbia and Ninth circuits of the U.S. Courts of Appeals, discussed in Chapter Four, are illustrative. In Yeager v. DEA, the D.C. Circuit held that agencies did not have a duty to use computer technology to edit computerized information to render it disclosable. The court reasoned that to do so constituted creation of a new record, which was not required of paper records.¹⁴ The Ninth Circuit reached a different conclusion in Long v. IRS, which held that editing computer tapes to make information disclosable did not constitute creation of a new record.¹⁵

Although courts have rendered conflicting opinions in cases involving technical and definitional issues, this confusion can be resolved by the legislative process. Congress, guided by the well-established principle of maximum openness, can revise guidelines and retool

definitions to reflect the realities of computerized information systems. Related recommendations will be offered at the end of this chapter.

The far more problematic access issue raised by the computerization of government information involves the nature of such information and whether its form, not its content, constitutes a greater threat to individual privacy. In Reporters Committee in 1989, the Supreme Court reasoned that government information stored in computers posed a greater privacy threat than the identical information scattered among public sources. Other court opinions, at various levels in the judicial system, have raised concern about information compiled in government data bases. But the Reporters Committee opinion provided an important difference. The Court opted for a bright line rule, reasoning that disclosure of certain categories of public information held in computers always constituted an undue privacy threat and could routinely be deemed an unwarranted privacy threat and be withheld without a case-by-case analysis. The language of Exemptions 6 and 7 of the Freedom of Information Act that requires a determination of whether a particular invasion of privacy was "unwarranted" had been interpreted as requiring a case-by-case determination. That interpretation allowed for a balancing of competing interests, whereby courts considered the privacy interests at stake versus the public benefit from disclosure.

The Court in Reporters Committee also held a seemingly narrow view of the public interest served by disclosure of government information, focusing only on information that had an obvious bearing on an agency's performance of its statutory duties. The Court said that since Congress had not provided the specific criteria in the FOIA for balancing a particular privacy interest with the public interest in disclosure, then courts should not try to do so.¹⁶

Generalized fears about the dangers computers pose to privacy appear to have influenced the Court's reasoning in Reporters Committee. If former levels of access are to be maintained, a method for balancing the competing interests of privacy and public access to government information that focuses on the content, not the form, of information is needed. To this end, a descriptive model is proposed to help identify a reasonable balance between privacy and public access. It draws on historical concepts of privacy and public access, on the writings of legal scholars and social scientists, and on the reasoning of various courts that have embraced the duty to engage in meaningful balancing.

A Model of Relative Values

Before a model is outlined, it is helpful to highlight the relative values of privacy and access. Alan Westin, whose writings and testimony permeated much of the legislative and judicial discussion of the notion of

informational privacy, has pointed out that privacy historically has been a relative concept, governed by the relative importance of ever-shifting social values. As he notes in his influential book Privacy and Freedom, "When the American Republic was founded, the framers established a libertarian equilibrium among competing values of privacy, disclosure, and surveillance. This balance was based on the technological realities of eighteenth-century life."¹⁷ The theme that privacy was a relative value lay the foundation for historian David H. Flaherty's assessment of privacy in Privacy in Colonial New England. In the introduction to his book, Flaherty proposed as his framework the balancing of privacy with competing values:

The heart of a study of personal privacy is the discovery of the balance of interests affecting privacy in a society. Since too much or too little privacy produces imbalance, every society has processes at the individual and societal levels for adjusting such competing values as privacy, companionship, compulsory disclosure, and physical surveillance. The well-balanced personality displays all of these factors in equilibrium with the limits of the environmental conditions and social norms of his society.¹⁸

The Privacy Protection Study Commission, established by the legislation creating the Privacy Act of 1974, echoed the theme that privacy is a relative concept that "does not and cannot exist in a vacuum." In its 1977 report on the state of privacy with respect to government information systems, titled Personal Privacy in an Information Society, the commission recognized that how agencies gathered and

disseminated information affected such values as access. Under the heading "Competing Public-Policy Interests," the commission noted,

A major theme of this report is that privacy, both as a societal value and as an individual interest, does not and cannot exist in a vacuum. Indeed, "privacy" is a poor label for many of the issues the Commission addresses because to many people the concept connotes isolation and secrecy, whereas the relationships the Commission is concerned with are inherently social. Because they are, moreover, the privacy protections afforded them must be balanced against other significant societal values and interests. The Commission has identified five such competing societal values that must be taken into account in formulating public policy to protect personal privacy: (1) First Amendment interests; (2) freedom of information interests; (3) the societal interests in law enforcement; (4) cost; and (5) Federal-State relations.¹⁹

Common to these assessments of privacy is the observation that it is among many values that interact in society and that at times must be balanced with competing interests. And so, for the purposes of this project, the model proposed will focus on two intertwined values supporting access identified by the Privacy Protection Study Commission: First Amendment interests and freedom of information interests, both of which form the underpinnings of a right of access.

The project will attempt to set up a circle of values supporting public access, with immutable values at its core, followed by decreasing values that tend to be more susceptible to societal changes and more likely to yield to competing social values. A similar circle will be

established for privacy values, with core values at the center, followed by decreasing values that are more likely to yield to competing societal interests. Values at each circle's center are referred to as "core" values because that is the term used by several social scientists who have studied a range of privacy values.²⁰

Legal scholar Charles Fried has provided a useful example that shows how privacy values might flow from one ring to the next. Fried, using the example of an illness, noted,

We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details. For instance, a casual acquaintance may comfortably know that I am sick, but it would violate my privacy if he knew the nature of the illness. Or a good friend may know what particular illness I am suffering from, but it would violate my privacy if he were actually to witness my suffering from some symptom which he must know is associated with the disease.²¹

In the model, access and privacy will be approached using the process suggested by Justice Goldberg in his concurrence in Griswold v. Connecticut of looking "to the tradition and [collective] consciousness of our people [and at] the totality of the constitutional scheme under which we live."²² Little attempt is made to distinguish between statutory and constitutional foundations for the particular value. Instead, focus is on the potential for societal benefit or for personal harm. The model assumes the closer a value is to the core, the more weight it should be given when balancing that value with a competing social interest.

The works of several social scientists are useful for relating privacy values to competing social values. Kurt Lewin, R.E. Park, and Ervin Goffman have described privacy in terms of concentric rings, surrounding a core value of privacy.²³ Values in the various rings of the circles resemble many of those discussed in the development of privacy in Chapter Two. As rings move farther from the core, they contain information that is less personal in nature and is less likely to cause unwarranted harm. How close particular information is to the privacy core is not static but depends largely on changes in a range of social values. In other words, personal information could shift from ring to ring over time, as societal values evolve.

It should be underscored that the proposed model is descriptive, attempting to show the relative weight of privacy and access within their respective circles. Consequently, a Second Ring privacy value might not always have the identical weight of a Second Ring access value. Ultimately, effective balancing would have to take into account all circumstances and would require, to some extent, the subjective assignment of a privacy or access interest to a particular ring.

Relative Privacy Values

Core Privacy Values

Core privacy values consist of individuals' innermost thoughts, feelings, and sentiments. Lewin, Park, and

Goffman describe these as individuals' "ultimate secrets-- those hopes, fears, and prayers that are beyond sharing with anyone" unless an individual chooses to do so.²⁴ Government files contain little, if any, of this kind of information because of strict constitutional and statutory limitations on its collection and because the information is the kind people rarely give up freely. The Constitution contains prohibitions against compelled and self-incriminating speech when the result could be potential harm to the speaker.²⁵ Even when compelled speech is allowed (such as in a criminal trial setting), it is subject to rigid limitations. To the extent that this kind of information exists in government records outside of public trial settings, intimate information is well protected from disclosure by statutes.²⁶

Second Ring Privacy Values

The next ring contains intimate information, the disclosure of which could lead to some kind of harm to an individual. Westin, drawing on the work of the social scientists mentioned previously, describes this as "intimate secrets . . . that can be willingly shared with close relations, confessions, or strangers who . . . cannot injure."²⁷ These values are much like those expressed by John Adams in Chapter Two. Said Adams, "Things that ought to be communicated to some of our Friends, that they may improve them to our Profit and Honour or Pleasure, should be concealed from our Enemies, and from indiscreet friends."²⁸

Several socially and legally recognized common law privileges resemble these values. They include privileged communications between wife and husband, priest and penitent, lawyer and client, and doctor and patient. The Supreme Court recognized the privacy of intimate decision making in Griswold v. Connecticut²⁹ and Roe v. Wade,³⁰ which dealt with decisions about birth control and abortion, respectively. The Court also recognized informational privacy rights in Whalen v. Roe, a case that involved the issue of doctor-patient relationships. The Court concluded that the Constitution did not bar government from collecting such information and storing it in a computer data base. The Court did, however, state that when government collected such personal data, it had a concomitant duty to ensure its security.³¹ Like information implicating core privacy values, Second Ring values are generally well shielded from unwarranted disclosure by statutes.³²

Third Ring Privacy Values

This ring contains personal information that is open to members of the individual's friendship group. The ring also contains information on group affiliation, which the Supreme Court recognized in Shelton v. Tucker and NAACP v. Alabama. In Shelton v. Tucker, the Court struck down an Arkansas statute requiring teachers to disclose organizations to which they belonged. The Court reasoned that mandatory disclosure of membership in unpopular or controversial

organizations could lead to harm to an individual.³³ The Court reached a similar conclusion in NAACP v. Alabama, which overturned a court order compelling the civil rights organization to turn over membership rolls to the state.³⁴ In both cases, the individuals or organizations may voluntarily disclose their membership but may not be compelled to do so.

Fourth Ring Privacy Values

This ring contains personal information that individuals give up as part of their day-to-day interaction with society, much of which becomes a part of the public record or is publicly available from other sources. In most cases, the information is given voluntarily, or in exchange for certain government-related rights and benefits, with the understanding that the individual is relinquishing complete control of the information. However, some disclosure of information is compelled by government, as when individuals become involved in the judicial system. Information is given to government and other entities for a variety of reasons. For example, individuals relinquish personal information when they form a corporation or license a business, receive a driver's license, sell or purchase houses, get married or divorced, subscribe to municipal utilities, seek government benefits, seek a permit for a government-regulated activity, and interact with the judicial system. This kind of information traditionally has

been part of the public record. In many cases, such information has become accessible under the common law with little privacy interest attached. Such information also has been recognized as part of the public record by a raft of federal and state access legislation, unless exempted by statute.

Fifth Ring Privacy Values

This level contains information that individuals freely disclose to government or businesses or otherwise relinquish with little expectation of privacy or fear of harm, such as telephone directory or city directory information or information such as names and addresses voluntarily disclosed for commerce purposes. Mailing lists based on magazine subscriptions or donations to charitable organizations are an example.

Relative Access Values

Establishing a clear core value supporting public access is more problematic than with privacy because the benefit of such access cannot be defined in terms of a single, individual right, such as personal "liberty." In fact, access is difficult to explain in terms of individual liberties because the very concept of access, when it involves personal information, depends on the individual relinquishing certain rights and interests for the benefit of society as a whole. While most of the Bill of Rights reflects the libertarian sentiments of the Founders'

generation with its focus on individual rights, access is predicated more on the theory of commonwealth, or the belief that individuals in a society must relinquish some rights and freedoms for the benefit of society at large.³⁵

Perhaps delineating the core value of access can best be achieved by attempting to answer the following question: What purpose did the Founders have in mind when they established a democratic government, one that depended for existence on the knowledge and consent of the people? While there obviously is no single answer to this question, it could be inferred from the writings of the Founders' generation and subsequent interpretations that the Founders envisioned a government that would take its direction from an informed citizenry, not a government that acted independent of the public it represented.

Following this reasoning, it could be surmised that the core value supporting access to government information is, as Alexander Meiklejohn has argued, the need for an informed citizenry in the process of self-governance. This reasoning, which Meiklejohn saw as the primary function of the First Amendment, was underscored by the Supreme Court's landmark opinion in New York Times v. Sullivan. In Sullivan, the Court held that the need for the free discussion of ideas in a democratic society was paramount to the individual rights of public officials to sue for libel, absent evidence that the press knew certain information was

incorrect or acted recklessly with regard to the truth or falsity of the information.³⁶ To the Court, the free exchange of information and ideas in society was so important that it superseded the rights of some individuals in some circumstances.

The Supreme Court has recognized the general need for an informed citizenry in a range of cases, dealing with information not solely related to the performance of government. In Virginia Pharmacy, for example, the Court held that the free flow of commercial information was essential to society--information that only indirectly informed the citizenry with respect to self-governance.³⁷ Similarly, the Court held that corporate speakers contributed to public discourse on important issues and, therefore, could not be restrained simply because their voices might be more powerful.³⁸ And in Richmond Newspapers, members of the Court agreed American society depended on government openness if members of society were to remain confident in the democratic process, at least with respect to the judicial system.³⁹

Most federal and state access legislation mandates disclosure of nonexempt information without regard for the reason the information is being sought. But when access is questionable and legal challenges arise, the reason information is sought sometimes becomes important when balancing privacy and public interest. The Freedom of

Information Act, which requires no reason for routine access, nonetheless looks at the reason for access when assessing access fees.⁴⁰ Generally, fees are waived or reduced when access is in the public interest, that is, when it enhances the flow of important information to society. In other words, the fee structure recognizes the necessity of the flow of government information into a democratic society and makes allowances to facilitate this flow. For example, fee relief is provided when information is sought for academic purposes or in the preparation of news reports and analysis.

What the preceding suggests, along with legislative recognition of a right of access that balances privacy interests with interests served by disclosure of government information, is an access circle with the fundamental need for an informed citizenry as its core value. From James Madison and Thomas Jefferson to the twentieth century's Vincent Blasi, it has been underscored that the most important information for American citizens to have is what their government is doing. The proposed circle takes into consideration the reasons information is sought, inasmuch as those reasons might have a bearing on how that information affects society. Various legislation, as well as several court cases that have attempted to balance privacy and access, help define the rings surrounding this core value.

Core Value for Access

The core value in the access circle comprises information that is essential for society to understand and assess the workings of government. Disclosure of this kind of information is similar to duty the Supreme Court recognized in Reporters Committee as fulfilling the public interest within the meaning of the Freedom of Information Act.⁴¹ But, unlike Reporters Committee, which contemplated access only to information that reflected directly on the statutory duties of a particular agency, this ring would include all information that related to the operation of government. Indeed, it would include the very information at question in Reporters Committee criminal history information on a reputed organized crime figure involved in a legitimate business with ties to a corrupt congressman. For example, journalists might be able to analyze computerized arrest records, which contain personal information such as names, and compare them to records of owners of corporations that do business with the government. In this case, the information as disclosed might reveal little or nothing about each agency's statutory duties. But, when analyzed together, the result might have much to say about some important aspect of government.

Second Ring Access Values

The Second Ring value access circle comprises information not directly about government but that

contributes to understanding government or facilitates the political process. This ring of access is close to the core but separated slightly because it acknowledges indirect effects, or benefits, disclosure might provide to society beyond merely disclosing agency activity. In this ring, the purpose for which information was sought might become relevant. The ring would encompass much of the routine information government gathers and stores because independent analysis of such information for various reasons could reflect on how government goes about the people's business. The analysis might not reflect on the performance of the particular agency that had the information but might, instead, be related to some past or future executive decision or public policy. A case that acknowledged the indirect, or secondary, effect of disclosure is Columbia Meat Packing Co. v. Department of Agriculture, in which the First Circuit of the U.S. Court of Appeals ordered disclosure of the names of two meat inspectors convicted of taking bribes in a widespread scandal in the meat processing industry. The court reasoned that information about the individual careers of the inspectors alone was of little public interest but that disclosure served a broader interest in preventing future scandals.⁴²

Third Ring Access Values

The Third Ring value in the access circle comprises information not directly about government but the disclosure

of which facilitates understanding of social and other issues that, in the collective, contribute to the process of self-governance. At this level, the purpose for which information is sought also might become important in assessing the societal value of disclosure. For example, in the case, International Brotherhood of Electrical Workers No. 5 v. Department of Housing and Urban Development, the Third Circuit of the U.S. Court of Appeals reasoned that release of names and addresses of people employed under a federal statute, which implicated minor privacy interests, served the public interest since such disclosure could make contractors more likely to abide by terms of the statute.⁴³

Fourth Ring Access Values

The Fourth Ring value in the access circle comprises information sought by individuals or other interests that add value to the information and disseminate it in such a way that it benefits society. Value is added when information is analyzed, organized, packaged, or otherwise made more understandable and useful to members of society. At this level, the purpose of disclosure also could be important in assessing the societal benefit of information. Many commercial information vendors and public- and special-interest groups seek government information to package and analyze for a range of useful and socially valuable purposes. Some of this information contains personal data, such as the names and addresses of government retirees. It

would be disclosable because disclosure could lead to their receiving information that might benefit them at minimal risk of privacy loss. A federal district court applied such reasoning in National Association of Retired Federal Employees v. Horner when it allowed disclosure of names and addresses of persons added to federal annuity rolls. The district court said any privacy infringement would be minor and that "the public interest in disclosure flows from the NARFE's service and the fact that many annuitants might be pleased to learn of them."⁴⁴ (In the wake of the Supreme Court's opinion in Reporters Committee, however, the D.C. Circuit of the U.S. Court of Appeals reversed the lower court on the basis of narrowed definition of public interest in disclosure. Since a privacy interest, even a minimal one, was at stake and disclosure would reveal nothing about the conduct of agency duties, privacy should prevail, the Court reasoned.)⁴⁵

The kind of access described in the Fourth Ring increases the flow of information to society or helps target the information to those who might find it most useful. When viewed collectively over time, this increased flow contributes to an informed citizenry. The Supreme Court in Virginia Pharmacy recognized a similar value when the Court reasoned that public knowledge of drug pricing ultimately could affect public policy regarding regulation of the prescription drug industry.⁴⁶

Fifth Ring Access Value

The Fifth Ring value in the access circle comprises information sought for personal reasons. Single instances of this kind of access contribute little that is obvious to public understanding of government and society. Yet, cases of individual access, in the aggregate and over time, do facilitate understanding of government and social issues and therefore have social value.

Sixth Ring Access Values

The Sixth Ring value in the access circle comprises information sought for for profit reasons alone. This might include names and addresses sought for commercial mailing lists, etc. In some cases, such disclosure might result in a measurable societal benefit that would enhance its disclosure value. However, in many instances the public interest in disclosure could be mitigated by the purely commercial message and the nature of the proposed transaction. Several court cases have suggested this is a low access value that can be overcome by minor privacy values.⁴⁷

Application of the Model

An example to show how this descriptive model might prove helpful is Department of State v. Washington Post Co., a 1982 case involving attempts by the newspaper through the Federal Freedom of Information Act to determine whether two Iranian officials were U.S. citizens. The State Department

refused to disclose the information, citing Exemption 6 to the FOIA, which shielded personnel, medical, and "similar" files from unwarranted invasions of privacy. After hearing the arguments that disclosure might put the new citizens' lives at risk, the Supreme Court rejected the D.C. Circuit's assertion that privacy should be construed narrowly, reasoning instead that a broader definition of privacy was in order that included nonintimate information.⁴⁸ Under usual circumstances, information about citizenship, a status normally conferred on non-American-born individuals during a public ceremony, would have little privacy value and might fall into Ring Four of the privacy circle with other information from public proceedings. However, because of the United States' strained relations at that time with Iran over the holding of American hostages and subsequent U.S. retaliation, the new citizens might reasonably be expected to face some kind of physical danger not normally associated with disclosure of citizenship. That being the case, the privacy value of the information--necessary to the physical well-being of the individuals--would move to the Third Ring or even Second, thereby shifting the balance away from disclosure. In effect, this is what the Supreme Court did in the case. To resolve the personal danger issue, the Court focused not on the nature of the information, which had at least an indirect bearing on public policy, but on its potential to cause harm, assigning to it a higher

privacy value as a result. Unfortunately from a pro-access perspective, to achieve the desired result, the Court resorted to expanding an FOIA exemption to include nonintimate information in order to meet the needs of a particular case.

The model also could be applied to a case the Court agreed to hear during the 1993 term. The case, Federal Labor Relations Authority v. U.S. Department of Defense, involves an attempt by a federal employees union to obtain names and addresses of employees of federal agencies.⁴⁹ The Fifth Circuit of the U.S. Court of Appeals held that the agencies must disclose the information under terms of the Federal Service Labor-Management Relations Statute to ensure "full and proper conduct of collective bargaining."⁵⁰ Under the proposed privacy/access circles, the names and addresses--information most employees likely had turned over to published commercial directories and disclosed freely in daily commerce--would likely fall into privacy Ring Five, having limited privacy value. On the access side, the statutory recognition of such access and its role in collective bargaining might place the access value in the Third Ring. Under this analysis, the privacy value of the information is low (distant from the core) and the public interest sufficiently high (closer to the core) to warrant disclosure.

The model produces interesting results when applied to the Reporters Committee case itself. Recall that the case ultimately focused on a request by a CBS correspondent and the Reporters Committee for Freedom of the Press for public-record criminal history information. The information was about a principal in a company identified by the Pennsylvania Crime Commission as a legitimate business dominated by organized crime that had dealings with a corrupt United States congressman. Assuming that the information were arrest records--a part of the public records in some jurisdictions--the information might fall in Ring Four of the privacy model. This kind of information normally retains limited privacy value, and the public interest in criminal activities would be high. Accordingly, the value for access would fall into the Second Ring. When the fact the subject of the information had been linked to an alleged corrupt congressman is taken into account, the values supporting access would be magnified, shifting it to the core value for access since the law-making process itself was implicated. Under this analysis, the information should have been disclosed notwithstanding its personal nature and presence in a computer data base.

Obviously, in some instances the values of access and privacy would appear equal. While the model still would be useful in clarifying the issues and exposing unreasonable or emotional concerns, ultimately courts would have to do what

they have always done--reach the best solution given the individual circumstances of the case.

The Need for a Response

The preceding model attempts to describe how the balance--however imperfect--between privacy and access has developed and worked over time based on the content of information and its potential for personal harm. However, as some of the computer/access cases discussed previously have shown, the relationship between access and privacy has become clouded when computer fears are raised. The seeds for computer/privacy concerns were planted long ago, in the 1960s, when the dangers that might arise from the misuse of computers formed the centerpiece of important public policy debates over government information practices. These concerns took form in the Supreme Court's Reporters Committee opinion in ways that could curtail access as the Court shifted its focus to the computerized form of the information, not the content of the information and the effect its disclosure might have on society. The Supreme Court's recognition of enhanced dangers from computerized information--even when it had minimal privacy values--echoed the legal reasoning of some lower courts.

As computers confound existing access laws and as court opinions send out mixed signals to custodians and access-seekers alike, it again becomes clear that a carefully reasoned legislative remedy is needed if public and press

access are to continue at traditional levels in the age of computers.

There are risks in tampering with the Freedom of Information Act and other access legislation. Statutes generally have worked to streamline the flow of information to society, and any effort to revisit legislation is in danger of being diverted by emotional and exaggerated privacy concerns. For example, the ongoing criticism of information vendors, or credit bureaus, in the popular press has affected public opinion and pushed privacy fears onto center stage, according to several polls. Even though commercial data vendors operate in the private sector, legislation to address this worry easily could be overbroad and could muddy the waters of any revisitation of the FOIA.

Yet, these risks are worth taking. Computers are going to continue to proliferate and, along with them, other new technologies that will challenge old policies and ways of doing things. If Congress does not begin to grapple with the privacy/access equation now, how much more difficult will it be 10 years hence? Congress must review the purpose of the FOIA by responding at two levels; in both instances, updating of access legislation should be guided by the philosophy of maximum disclosure.

First, Congress can deal with the technical and definitional problems affecting access to ensure that

technology facilitates, not frustrates, access. To accomplish this, several recommendations are offered:⁵¹

Congress and state legislatures should mandate that agencies introducing computers or upgrading them make public access a priority. This requires that computer hardware and software be designed to facilitate access and that record keepers be properly trained.

Once systems are properly designed and personnel properly trained, legislators should redefine the access-related terminology and definitions to reflect the realities of computerized information systems. It should be made clear to record keepers what tasks are expected of them to ensure that computers are used to maximize access.

Second, Congress and legislatures need to address access legislation on the second, more problematic level. This involves the nature of computerized information and whether it poses an inherently greater threat to personal privacy than the same information in paper form. Congress has dealt with this issue before, when it resisted arguments that certain kinds of computerized information, for reasons including privacy, should be classified "sensitive" and disclosure limited simply because of its easy accessibility in computers. The legislative history of the Computer Security Act, discussed in Chapter Three, made clear that any "sensitive" designation of computerized records could not be used to foreclose access mandated under the Freedom

of Information Act.⁵² But the Supreme Court's conclusion in Reporters Committee that some classes of computerized records could routinely be deemed unwarranted privacy threats without a case-by-case balancing has potentially the same effect as the attempt to create a "sensitive" designation. Congress needs to clarify this issue to ensure that the FOIA remains guided by a philosophy of maximum agency disclosure and that the content of information, not its form, determines access.

This is not to suggest that all personal information in government possession should be freely accessible; the Privacy Act, the FOIA exemptions, and other legislation spell out the government's responsibility to protect certain privacy interests. Indeed, asserting the privacy rights of individuals about whom government gathers and stores information is a potent public policy rationale for restricting access, as illustrated in Chapters Three and Four. And the political attractiveness of that rationale has been heightened by the concern over the mishandling of information by commercial vendors that share personal information for a fee.⁵³

Legislation is important at this juncture to ensure access is not reduced simply because of generalized concerns about computers or because agency personnel may be unwilling or unable to use the new technology for a greater societal good. Revisiting public access laws--by state legislatures

as well as by Congress--will provide the chance to acknowledge the capabilities of computers while ensuring these capabilities are used to both ensure privacy and to enhance, not frustrate, public access.

Notes

1. Howard Kurtz, "Reporters Let Their Terminals Do the Walking," The Washington Post, July 7, 1991, at F4.
2. See Vincent Blasi, "The Pathological Perspective and the First Amendment," 85 Colum. L. Rev. 449 (1985).
3. See Arthur Miller, The Assault on Privacy (1971); William Prosser, "Privacy," 48 Calif. L. Rev. 383 (1960).
4. U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).
5. See National Labor Relations Board v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).
6. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).
7. U.S. Const. art. I, sec. 5.
8. See Alexander Meiklejohn, Free Speech and Its Relation to Self-Government (1948); New York Times v. Sullivan, 376 U.S. 254 (1964).
9. Blasi, supra note 2, at 527, 529-544.
10. Houchins v. KOED, 438 U.S. 14-15 (1975).
11. Id.
12. S. Rep. No. 813, 89th Cong., 1st Sess., at 3, cited in GTE Sylvania, Inc. v. Consumers Union, 445 U.S. 375, 385 (1979).
13. Yeager v. DEA, 678 F.2d 315, 326-327 (D.C. Cir. 1982)
14. Id.
15. Long v. IRS, 596 F.2d 362 (9th Cir. 1979).
16. Supra note 4.

17. Alan Westin, Privacy and Freedom 67 (1967).
18. David H. Flaherty, Privacy in Colonial New England 18 (1972).
19. Privacy Protection Study Commission, Personal Privacy in an Information Society 21 (1977).
20. Westin, Privacy and Freedom at 33.
21. Charles Fried, "Privacy," 77 Yale L. J. 477-486 (1968).
22. Griswold v. Connecticut, 381 U.S. 479, 494 (1965) (Justice Goldberg, concurring).
23. Westin, Privacy and Freedom at 33.
24. Id.
25. U.S. Const. amend. I, V.
26. Press-Enterprise v. Riverside County Superior Court, 464 U.S. 501, 520 (1984) (Justice Marshall, concurring).
27. Westin, Privacy and Freedom at 33.
28. Flaherty, Privacy in Colonial New England at 5.
29. Griswold at 479.
30. Roe v. Wade, 410 U.S. 113 (1973).
31. Whalen v. Roe, 429 U.S. 592 (1977).
32. See generally the Privacy Act of 1974, 5 U.S.C. sec. 552a; and the nine exemptions to the Freedom of Information Act, 5 U.S.C. sec. 552(b) (1), (2), (3), (4), (5), (6), (7), (8), (9).
33. Shelton v. Tucker, 364 U.S. 479 (1960).
34. NAACP v. Alabama, 357 U.S. 449 (1958).
35. Kermit Hall, The Magic Mirror: Law in American History 62, 94-95 (1989).
36. New York Times v. Sullivan at 270.
37. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

38. First National Bank of Boston v. Bellotti, 435 U.S. 756 (1978).
39. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).
40. Freedom of Information Act, 5 U.S.C. 552 (1966).
41. Reporters Committee at 733.
42. Columbia Meat Packing Co. v. Department of Agriculture, 563 F.2d 495 (1st Cir. 1977).
43. International Brotherhood of Electrical Workers No. 5 v. Department of Housing and Urban Development, 852 F.2d. 87, 90 (3rd Cir. 1988).
44. National Association of Retired Federal Employees v. Horner, 633 F.Supp. 1241 (D.D.C. 1986).
45. National Association of Retired Federal Employees v. Horner, 879 F.2d 873 (D.C. Cir. 1989).
46. Virginia State Board of Pharmacy at 748.
47. See generally Minnis v. Department of Agriculture, 737 F.2d. 784, 786-787 (9th Cir. 1984); Wine Hobby USA, Inc. v. IRS, 502 F.2d 133, 137 (3rd Cir. 1974).
48. Department of State v. Washington Post Co., 456 U.S. 595 (1982).
49. Federal Labor Relations Authority v. U.S. Department of Defense, 975 F.2d 1105 (1992).
50. Id. at 1109.
51. Matthew D. Bunker, Sigman L. Splichal, Bill F. Chamberlin, and Linda Perry, "Access to Government-Held Information in the Computer Age," 20 Fla. St. U.L. Rev. 596-598 (Winter 1993).
52. Computer Security Act of 1987, Pub. L. No. 100-235.
53. See "How Did They Get My Name? Consumers are growing more uneasy about threats to privacy--and are fighting back," Newsweek, June 3, 1991, at 40; Peter Kerr, "Big Credit Bureau to Let Consumers See Reports Free: A Response to Criticism; TRW Acts as Industry Faces Mounting Pressure Over Errors in Its Records," The New York Times, October 15, 1991, at 1; Leonard Sloane, "Just Who Can Raise

the Shades and Peek into Private Matters: A group seeks new ways to keep my business from becoming yours," The New York Times, January 25, 1992, at 16.

BIBLIOGRAPHY

Legal Citations

- Abrams v. United States, 250 U.S. 616 (1919).
- Allgeyer v. Louisiana, 165 U.S. 578 (1897).
- American Federation of Government Employees vs. Department of Health and Human Services, No. 89-444 (1989).
- Asbury Park Press, Inc. v. Department of Health, 558 A.2d 1363 (N.J. 1989).
- Beacon Journal Publishing Co. v. Andrews, 358 N.E.2d 565 (December 1976).
- Bowie v. Evanston Community Consolidated School District No. 65, 538 N.E.2d 557 (April 20, 1989).
- Boyd v. United States, 116 U.S. 616 (1886).
- Branzburg v. Hayes, 408 U.S. 655 (1972).
- Brown v. FBI, 658 F.2d 71 (2d Cir. 1981).
- Burrows v. Superior Court, 529 P.2d 590 (1974).
- Burton v. Tuite, 78 Mich. 363 (1889).
- Clarke v. U.S. Department of Treasury, Civ. A. No. 84-1873 (E.D. Pa. 1986).
- Clement v. Graham, 78 Vt. 290 (1906).
- Cochran v. United States, 770 F.2d 949 (11th Cir. 1985).
- Columbia Packing Co. v. Department of Agriculture, 563 F.2d 495 (1st Cir. 1977).
- Davidson v. Dill, 503 P.2d 157 (1972).
- Demay v. Roberts, 46 Mich. 160, 9 N.W. 146 (1881).

Dennis v. United States, 341 U.S. 494 (1951).

Department of Air Force v. Rose, 425 U.S. 352 (1976).

Doe v. Registrar of Motor Vehicles, 528 N.E.2d 880 (1988).

Environmental Protection Agency v. Mink, 410 U.S. 73 (1973).

Family Life League v. Department of Public Aid, 493 N.E.2d 1054 (May 21, 1986).

Fayette Co. v. Martin, 279 Ky. 387, S.W.2d 838 (1939).

First National Bank v. Bellotti, 435 U.S. 765 (1978).

Florida Star v. B.J.G., 109 S. Ct. 2603 (1989).

Forsham v. Harris, 445 U.S. 169 (1980).

Gitlow v. New York, 268 U.S. 652 (1925).

Globe Newspaper Co. v. Superior Court, 457 U.S. 596 (1982).

Goldman v. United States, 316 U.S. 129 (1942).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Grosjean v. American Press Co., 297 U.S. 233 (1936).

Igneri v. Moore, 721 F.Supp. 406 (N.D.N.Y. 1989).

In re Mack, 368 Pa. 251 (1956).

International Board of Electrical Workers v. Department of Housing and Urban Development, 852 F.2d 87 (3d Cir. 1988).

Katz v. United States, 389 U.S. 347 (1967).

Kestenbaum v. Michigan State University, 327 N.W.2d 783 (1982).

Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136 (1980).

Kryston v. Board of Education, East Rampao Central School District, 430 N.Y.S.2d 688 (August 11, 1980).

Lead Industry Ass'n v. OSHA, 610 F.2d 70 (2nd Cir. 1979).

Lloyd & Henninger v. Marshall, 526 F. Supp. 485 (M.D. Fla. 1981).

- Long v. IRS, 596 F.2d 362 (9th Cir. 1979).
- MacEwan v. Holm, 226 Or. 27 (1961).
- Maher v. Freedom of Information Commission, 472 A.2d 321 (Conn. Feb. 21, 1984).
- Mapp v. Ohio, 367 U.S. 644 (1961).
- Martin & Merrell, Inc. v. United States Custom Service, 657 F.Supp. 733 (S.D. Fla. Nov. 1986).
- Mead Data Cent., Inc. v. Department of Air Force, 566 F.2d 242 (D.C. Cir. 1977).
- Meyer v. Nebraska, 262 U.S. 390 (1923).
- Miami Herald v. Tornillo, 418 U.S. 241 (1974).
- Minnis v. Department of Agriculture, 737 F.2d 784 (9th Cir. 1984).
- Mullin v. Detroit Police, 348 N.W.2d 708 (1984).
- Multnomah County Medical Society v. Scott, 825 F.2d 1410 (9th Cir. 1987).
- NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).
- National Ass'n of Retired Federal Employees v. Horner, 879 F.2d 873 (D.C. Cir. 1989).
- Near v. Minnesota, 283 U.S. 697 (1931).
- Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976).
- New York Times v. Sullivan, 376 U.S. 254 (1964).
- NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978).
- NLRB v. Sears, Roebuck & Co., 421 U.S. 132 (1975).
- Olmstead v. United States, 227 U.S. 438 (1928).
- Paul v. Davis, 424 U.S. 693 (1976).
- Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).
- Pell v. Procunier, 417 U.S. 817 (1974).
- Pierce v. Society of Sisters, 268 U.S. 510 (1925).

Planned Parenthood of Southeastern Pennsylvania v. Casey, 60 U.S.L.W. 4795 (1992).

Poe v. Ullman, 367 U.S. 497 (1961).

Pope v. Curl, 2 Atk. 324, 26 Eng. Rep. 608 (1741).

Press Enterprise Co. v. Riverside County Superior Court, 464 U.S. 501 (1984).

Red Lion Broadcasting v. FCC, 395 U.S. 367 (1969).

Richmond Newspapers v. Virginia, 448 U.S. 555 (1980).

Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).

Roe v. Wade, 410 U.S. 113 (1973).

Saxbe v. Washington Post Co., 417 U.S. 843 (1974).

Schuyler v. Curtis, 15 N.Y. Supp. 787 (1891).

Shelton v. Tucker, 364 U.S. 479 (1960).

Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

Stanley v. Georgia, 394 U.S. 557 (1969).

State ex rel. Wellford v. Williams, 110 Tenn. 549 (1903).

Stephan v. Harder, 641 P.2d 366 (Kan. Feb. 17, 1982).

Sterline Drug, Inc. v. Harris, 488 F. Supp. 1019 (S.D.N.Y. 1980).

Stromberg v. California, 274 U.S. 359 (1931).

Szikszy v. Buelow, 436 N.Y.S.2d 558 (N.Y., Jan. 20, 1981).

United States v. Miller, 425 U.S. 435 (1976).

United States v. Nixon, 418 U.S. 683 (1974).

United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976).

Webb v. Shreveport, 371 S.2d 316 (1979).

Western Services, Inc. v. Sergeant School District No. RE-33J, 719 P.2d 355 (Colo. App. Jan. 2, 1986).

Whalen v. Roe, 429 U.S. 589 (1977).

Whitney v. California, 274 U.S. 357 (1927).

Wine Hobby USA, Inc. v. IRS, 502 F.2d 133 (3d Cir. 1983).

Yeager v. DEA, 678 F.2d 315 (D.C. Cir. 1982).

Books

Bayley, Edwin R. Joe McCarthy and the Press. Madison, Wis.: University of Wisconsin Press, 1981.

Bernstein, Jeremy. The Analytical Engine: Computers, Past, Present, and Future. New York: Random House, 1964.

Cohen, William, and John Kaplan. Constitutional Law: Civil Liberty and Individual Rights. 2nd ed. Mineola, N.Y.: The Foundation Press, Inc., 1982.

Cross, Harold. The People's Right to Know. New York: Columbia University Press, 1953.

De Sola Pool, Ithiel. Technologies of Freedom. Cambridge, Mass.: Belknap Press, 1983.

Emerson, Thomas. The Bill of Rights Today. New York: Public Affairs Committee, 1973.

_____. Toward a General Theory of the First Amendment. New York: Random House, 1963.

Emery, Michael, and Edwin Emery. The Press in America: An Interpretive History of the Mass Media. 6th ed. Englewood Cliffs, N.J.: Prentice-Hall, 1988.

Ernst, Morris L., and Alan U. Schwartz. The Right to Be Let Alone. New York: Macmillan Company, 1962.

Ferkiss, Victor C. Technological Man: The Myth and the Reality. New York: Braziller, 1969.

Flaherty, David. Privacy in Colonial New England. Charlottesville, Va.: University of Virginia Press, 1972.

Ford, Paul Leicester, ed. The Writings of Thomas Jefferson. New York: G.P. Putnam's Sons, 1892-1899.

- Fried, Charles. An Anatomy of Values. Cambridge, Mass.: Harvard University Press, 1970.
- Gettleman, Marvin E. The Great Society Reader: The Failure of American Liberalism. New York: Random House, 1967.
- Ginsberg, Eli. The Great Society: Lessons for the Future. New York: Basic Books, 1974.
- Griswold, Rufus W., ed. The Prose Works of John Milton. Vol. 1. Philadelphia: J.W. Moore, 1856.
- Hentoff, Nat. The First Freedom. New York: Delacorte Press, 1980.
- Hixson, Richard F. Privacy in a Public Society: Human Rights in Conflict. New York: Oxford University Press, 1987.
- Huxley, Aldous. Brave New World. New York: Bantam Books, 1958.
- Katsh, Ethan M. The Electronic Media and the Transformation of Law. New York: Oxford Press, 1989.
- Landis, Mark. Joseph McCarthy: The Politics of Chaos. London: Associated University Press, 1987.
- Levy, Leonard. Emergence of a Free Press. New York: Oxford University Press, 1985.
- _____. Jefferson and Civil Liberties: The Darker Side. Cambridge, Mass.: Harvard University Press, 1963.
- Locke, John. An Essay Concerning Human Understanding. London: Tegg and Co., 1952.
- Maslow, Abraham. Motivation and Personality. New York: Harper, 1954.
- _____. Religion, Values and Peak-Experience. New York: The Viking Press, 1970.
- Meiklejohn, Alexander. Free Speech and Its Relation to Self-Government. New York: Harper & Bros., 1948.
- Michael, Donald N. Cybernation: The Silent Conquest. Santa Barbara, Calif.: Center for the Study of Democratic Institutions, 1962.

- Middleton, Kent, and Bill F. Chamberlin. The Law of Public Communication. 2nd ed. New York: Longman Publishing Group, 1988.
- Mill, John Stuart. Considerations on Representative Government. C. Shields, ed. New York: Liberal Arts Press, 1958.
- _____. On Liberty. Boston: Ticknor and Fields, 1863.
- Miller, Arthur. The Assault on Privacy: Computers, Data Banks and Dossiers. Ann Arbor, Mich.: University of Michigan Press, 1971.
- Nader, Ralph. Unsafe at Any Speed: The Designed-In Danger of the American Automobile. New York: Grossman, 1965.
- Orwell, George. 1984. San Diego: Harcourt, Brace, and Co., 1949.
- Packard, Vance. The Naked Society. New York: D. McKay Co., 1964.
- Padover, Saul K., ed. The Complete Madison. New York: Harpster & Brothers, 1953.
- Paine, Thomas. The Rights of Man. New York: Penguin Books, 1984.
- Pember, Don R. Privacy and the Press. Seattle: University of Washington Press, 1972.
- Reporters Committee for Freedom of the Press. Tapping Official Secrets: A State Open Government Compendium. Washington, D.C.: Reporters Committee for Freedom of the Press, 1989.
- Rosenberg, Jerry M. The Death of Privacy. New York: Random House, 1969.
- Rostoker, Michael D., and Robert H. Rines. Computer Jurisprudence: Legal Responses to the Information Revolution. New York: Oceana Publications, Inc., 1986.
- Shattuck, John H.F. Rights of Privacy. Skokie, Ill.: National Textbook Co., 1977.
- Smith, Robert Ellis. Compilation of State and Federal Privacy Laws. Providence, R.I.: Privacy Journal, 1992.
- Tuchman, Barbara W. The March of Folly: From Troy to Vietnam. New York: Ballantine Books, 1984.

- Van Alstyne, William. Interpretations of the First Amendment. Durham, N.C.: Duke University Press, 1984.
- Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967.
- Westin, Alan F., and M. Baker. Databanks in a Free Society: Computers, Record-Keeping and Privacy. New York: Quadrangle Books, Inc., 1976.
- Wiggins, James R. Freedom or Secrecy? Oxford: Oxford University Press, 1964.
- Wilson, Woodrow. The New Freedom. New York: Doubleday, Page and Co., 1913.

Articles in Periodicals and Books

- Abrams, Floyd. "The Press Is Different: Reflections on Justice Stewart and the Autonomous Press." 7 Hofstra Law Review 563 (1979).
- Access Reports. Washington, D.C.: Plus Publications, Inc., November 29, 1989.
- Bazelon, David L. "Probing Privacy." 12 Gonzaga Law Review 587 (1977).
- Benjamin, Louise M. "Privacy, Computers, and Personal Information: Toward Equality and Equity in an Information Age." 13 Communications and the Law 3 (June 1991).
- Berman, Jerry J. "The Right To Know: Public Access to Electronic Public Information." 3 Software Law Journal 491 (Summer 1989).
- Blasi, Vincent. "The Checking Value in First Amendment Theory." 1977 American Bar Foundation Research Journal 521.
- _____. "The Pathological Perspective and the First Amendment." 85 Columbia Law Review 449 (1985).
- Brundy, D. "Computers and Smaller Local Governments." 12 Public Productivity Review 184 (1988).

- Bunker, Matthew D., Sigman L. Splichal, Bill F. Chamberlin, and Linda M. Perry. "Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology." 20 Florida State University Law Review 543 (Winter 1993).
- "Bureaucracy: Chains of Plastic." Newsweek, August 8, 1966, 27.
- Corcoran, Katherine. "Beating The Tape Resistance." News Inc., November 1991, 30.
- _____. "Power Journalists." News Inc., November 1991, 30.
- Dixon, David. "The Griswold Penumbra: Constitutional Charter for the Expanded Law of Privacy?" 64 Michigan Law Review 197 (1965).
- Fried, Charles. "Privacy." 77 Yale Law Journal 477 (1968).
- Goldman, Patti A. "The Freedom of Information Act Needs No Amendment to Ensure Access to Electronic Records." 7 Government Information Quarterly 389 (1990).
- Gorfinkel, John A., and Julian W. Mack II. "Dennis v. United States and the Clear and Present Danger Rule." 39 California Law Review 475 (1951).
- "A Government Watch on 200 Million Americans?" U.S. News & World Report, May 16, 1966, 56.
- Greenburg, M. "Uses of Computers in Organizations." Scientific America, Summer 1966, 192.
- Grodsky, Jamie A. "The Freedom of Information Act in the Electronic Age: The Statute Is Not User Friendly." 31 Jurimetrics Journal of Law, Science and Technology 17 (Fall 1990).
- Hartman, Mitchell. "Investigative Reporters Use Databases to Break Stories." The Quill, November/December 1990, 21-26.
- "How Computers Liven Management's Ways." Business Week, June 25, 1966, 15.
- Jaspin, Elliot, and Mark Sableman. "News Media Access to Computer Records: Updating Information Laws in the Electronic Age." 36 St. Louis University Law Journal 349 (1992).

Kalven, Harry. "Privacy and Tort Law--Were Warren and Brandeis Wrong?" 31 Law and Contemporary Problems 326 (1966).

_____. "The Problems of Privacy in the Year 2000." Daedalus 96 (Journal of the American Academy of Arts and Sciences 876, Summer 1967).

Kaplan, David A. "Is Roe Good Law?" Newsweek, April 27, 1992, 49-51.

Kirchner, J. "Latest Harris Poll Uncovers Mixed Attitudes About High Tech." Computerworld, Dec. 12, 1983, 1.

Linowes, David. "Must Privacy Die in the Computer Age?" 65 American Bar Association Journal 1180 (1979).

Macy, John W., Jr. "The Cybernation Generation." Time, April 2, 1965, 84.

Miller, Arthur. "Computers, Data Banks and Individual Privacy: An Overview." 4 Columbia Human Rights Law Review 1 (1972).

_____. "The National Data Center and Personal Privacy." The Atlantic, November 1967, 53.

_____. "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society." 67 Michigan Law Review 1091 (1969).

Miller, Richard I. "Data Banks and Privacy." Computers and the Law: An Introductory Handbook. Robert Pratt Bigelow, ed. 2d ed. Chicago, Ill.: Commerce Clearing House, 1969.

"The New Computerized Age." Saturday Review, July 23, 1966, 15.

Pfeiffer, J. "How Computers Will Change Your Life." McCall's, May 1965, 34.

Prosser, William. "Privacy." 48 California Law Review 383 (1960).

"Public Inspection of State and Municipal Executive Documents: Everybody, Practically Everything, Anytime, Except. . . ." 45 Fordham Law Review 1105 (1977).

Quinn, Jane Bryant. "Guarding Your Good Name." Newsweek, August 12, 1991, 64.

- Rehnquist, William. "Is An Expanding Right of Privacy Consistent with Fair and Effective Law Enforcement?" Nelson Timothy Stephens Lectures, University of Kansas Law School, September 26-27, 1974, 13 (Part One).
- Reid, T.R. "Computerthink." 5 APF Reporter 3 (Winter 1983).
- Ruggles, Richard. "On the Needs and Values of Data Banks." In "Symposium--Computers, Data Banks, and Individual Privacy." 53 Minnesota Law Review 211 (1968).
- Schwartz, John. "Consumer Enemy No. 1." Newsweek, October 28, 1991, 42.
- _____. "How Did They Get My Name?" Newsweek, June 3, 1991, 40.
- "Sharp Increase in Concern." 16 Privacy Journal 7 (May 1990).
- Soma, John T., and Richard A. Wehmhoefer. "A Legal and Technical Assessment of the Effects of Computers on Privacy." 60 Denver Law Journal 451 (1983).
- Sorokin, Leo T. "The Computerization of Government Information: Does It Circumvent Public Access Under the Freedom of Information Act and the Depository Library Program?" 24 Columbia Journal of Law & Social Problems 267 (1990).
- Southard, C. Dennis IV. "Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information." 9 Computer/Law Journal 359 (Summer 1989).
- Stewart, Potter. "Or of the Press." 26 Hastings Law Journal 631 (1975).
- Strong, Donsia Renee. "The Computer Matching and Privacy Protection Act of 1988: Necessary Relief from the Erosion of the Privacy Act of 1974." 2 Software Law Journal 391 (Summer 1988).
- Susman, Thomas M. "Introduction to the Issues, Problems and Relevant Law" in "Your Business, Your Trade Secrets, and Your Government." 34 Administrative Law Review 117 (1982).

- _____. "The Privacy Act and Freedom of Information Act: Conflict and Resolution." 21 John Marshall Law Review 703 (Summer 1988).
- Warren, Samuel D., and Louis Brandeis. "The Right of Privacy." 4 Harvard Law Review 193 (December 1890).
- Weingarten, Fred W. "Communications Technology: New Challenges to Privacy." 21 John Marshall Law Review 735 (1988).

Articles in Newspapers

- Hendricks, Evan. "How Not to Catch Welfare Cheaters." The Washington Post, July 1, 1979, C8.
- Kerr, Peter. "Big Credit Bureau to Let Consumers See Reports Free." The New York Times, October 15, 1991, 1.
- Kurtz, Howard. "Reporters Let Their Terminals Do the Walking." The Washington Post, July 7, 1991, F4.
- Landau, George, and Tim Novak. "Dead or Alive." St. Louis Post Dispatch, September 9, 1990, 1A.
- Sloane, Leonard. "Just Who Can Raise the Shades and Peek into Private Matters." The New York Times, January 25, 1992, 16.
- _____. "One-Stop Credit Report Covers Three Bureaus' Data." The New York Times, July 26, 1992, 50.
- "The Telephone Unmasked." The New York Times, October 12, 1877, 4.

Codes and Statutes

- Administrative Procedures Act, 5 U.S.C. sec. 1002 (1946).
- Cable Communication Policy Act, 47 U.S.C. sec. 521 (1984).
- Computer Crime Act, 18 U.S.C. sec. 1030 (1984). Amended by Pub. L. 99-473 (1986).
- Computer Fraud and Abuse Act, Pub. L. 99-474 (1986).
- Computer Matching and Privacy Protection Act, 5 U.S.C. sec. 552a(1988), reprinted in 1988 U.S. Code & Administrative News 3109.

- Computer Security Act, Pub. L. 100-235 (1987).
- Electronic Communications Privacy Act, 18 U.S.C. sec. 2510 (1986), reprinted in 1986 U.S. Code Congressional Administrative News 3555.
- Fair Credit Billing Act, 15 U.S.C. sec. 1666 (1976).
- Fair Credit Reporting Act, 15 U.S.C. sec. 1681 (1976).
- Family Educational Rights and Privacy Act, 20 U.S.C. sec. 1232 (1974).
- Federal Managers' Financial Integrity Act, 31 U.S.C. sec. 3512 (1982).
- Federal Records Act, 64 Stat. 583 (1950).
- Freedom of Information Act, 5 U.S.C. sec. 552 (1966).
- Indiana Open Records Law, Ind. Code sec. 5-14-3-1 (1977); Texas Stat. sec. 6252-17a.
- Privacy Act, 5 U.S.C. sec. 552a (1974), reprinted in 1974 U.S. Code Congressional & Administrative News 6926.
- Right to Financial Privacy Act, 12 U.S.C. sec. 3401 (1978).

Government Reports and Documents

- Ervin, Sam. 120 Congressional Record S12646-12650, May 1, 1974.
- General Services Administration, Federal Equipment Data Center. Automated Data Processing Equipment in the U.S. Government. Washington, D.C.: U.S. Government Printing Office, April, 1990.
- _____. Office of Federal Information Resources Management. Microcomputer Survey Report. Washington, D.C.: U.S. Government Printing Office, September, 1988.
- Mathias, Charles. 131 Congressional Record S2728-29, March 7, 1985.
- Office of Technology Assessment, U.S. Congress. Computer-Based National Information Systems. Washington, D.C.: U.S. Government Printing Office, 1981.

- _____. Electronic Record Systems and Individual Privacy. Washington, D.C.: U.S. Government Printing Office, 1986.
- Privacy Protection Study Commission. Personal Privacy in an Information Society. Washington, D.C.: U.S. Government Printing Office, 1977.
- _____. The Privacy Act of 1974: An Assessment. Washington, D.C.: U.S. Government Printing Office, 1977.
- Report of the Committee on the Preservation and Use of Economic Data to the Social Science Research Council. April 1965. Reprinted in House Hearings on Computers and Invasion of Privacy 195.
- Statistical Evaluation Report No. 6--Review of Proposal for a National Data Center. November 1965. Reprinted in House Hearings on Computers and Invasion of Privacy, 254.
- U.S. Department of Health, Education and Welfare. Records, Computers and the Rights of Citizens. Boston: The Massachusetts Institute of Technology, 1973.
- U.S. Department of Justice, Office of Policy Development. FOIA Update. Washington, D.C.: U.S. Government Printing Office, Spring 1989.

Government Hearings

- Computer Matching and Privacy Protection Act of 1986: Hearings Before the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs, 99th Cong., 2d Sess. (1986).
- Computer Matching and Privacy Protection Act of 1987: Hearings Before the House Committee on Government Operations, 100th Cong., 1st Sess. (1987).
- Computer Privacy: Hearings Before the Subcommittee on Administrative Practices and Procedures of the Senate Committee on the Judiciary, 90th Cong., 1st Sess. (1967).
- Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 92nd Cong., 1st Sess. (1971).

Invasion of Privacy: Hearings Before the Subcommittee on Administrative Practices and Procedures of the Senate Committee on the Judiciary, 89th Cong., 2d Sess. (1966).

Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs, 97th Cong., 2d Sess. (1982).

Privacy: The Collection, Use and Computerization of Personal Data: Joint Hearings Before the Subcommittee on Privacy and Information Systems of the Senate Committee on Government Operations and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, S. Rep. No. 1183, 93rd Cong., 2d Sess. (1974), reprinted in 1974 U.S. Code Congressional & Administrative News 6918.

The Computer and Invasion of Privacy: Hearings Before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations, 89th Cong., 2d Sess. (1966).

Unpublished Sources

Kostyu, Paul E. "Political Pressure: The Freedom of Information Act and John E. Moss Jr." Association for Education in Journalism and Mass Communication Southeast Colloquium, Orlando, Fla., February-March, 1991.

Kubrick, Stanley, director. 2001: A Space Odyssey. (Metro-Goldwyn-Mayer 1968).

Morrissey, David. "The Age of Electronic Government." Conference on Advanced Investigative Methods for Journalists, 1990.

Scott, Sandra Davidson. "Computer Technology v. Laws on Access." Association for Education in Journalism and Mass Communication, Boston, Mass., August, 1991.

BIOGRAPHICAL SKETCH

Sigman L. Splichal received B.S. and M.A. degrees from the University of Florida and worked as a newspaper reporter and editor in Georgia, Florida, and Virginia before returning to pursue a doctoral degree. Splichal's research interests focus on mass communication law and include issues related to newspaper management and ethics. He is an assistant professor at the University of Miami.

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Bill F. Chamberlin

Bill F. Chamberlin, Chairperson
Joseph L. Brechner Eminent Scholar
in Freedom of Information

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

William F. McKeen

William L. McKeen
Associate Professor of Journalism
and Communications

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Leonard P. Tipton


Leonard P. Tipton
Professor of Journalism and
Communications

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Kermit L. Hall

Kermit L. Hall
Professor of History

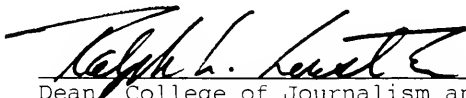
I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.



Fletcher Baldwin
Professor of Law

This dissertation was submitted to the Graduate Faculty of the College of Journalism and Communications and to the Graduate School and was accepted as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

August 1993



Dean, College of Journalism and
Communications

Dean, Graduate School

UNIVERSITY OF FLORIDA



3 1262 08553 5788